

计算方法丛书

快速数论变换

孙 琦 郑德勋 沈仲琦 著

科学出版社

计算方法丛书

快速数论变换

孙 琦 郑德勋 沈仲琦 著

科学出版社

1980

内 容 简 介

本书主要介绍快速数论变换的理论、方法、应用及其最新进展.

数论变换是把数论应用到数字处理中而得到的一种计算方法. 其特点是: (1)没有舍入误差; (2)其中某些变换比快速傅里叶变换还快. 它不仅在数字处理中有用,还可以应用到多项式、大整数相乘等方面的计算中去.

本书可供计算数学工作者、大专院校有关专业教师、研究生、高年级学生等参考.

计算方法丛书

快速数论变换

孙 琦 郑德勋 沈仲琦 著

*

科学出版社 出版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1980年 10 月第一版 开本: 850×1168 1/32

1980年 10 月第一次印刷 印张: 6 3/4

印数: 0001—12,230 字数: 172,000

统一书号: 13031·1286

本社书号: 1789·13—1

定价: 1.05 元

《计算方法丛书》编委会

前　　言

近年来，利用复数域上的离散傅里叶变换（DFT）对数字式信号进行处理，这种方法在雷达、通讯、遥感、物探、光学、医学等各方面都得到了有效的应用．特别是在1965年；Cooly和Tukey提出了快速计算离散傅里叶变换的算法——快速傅里叶变换（FFT），使得原来直接计算DFT的乘、加法次数的阶由$O(N^2)$降为$O(N\log_2 N)$，从而大大节省了计算量．这一方法促进了数字信号处理的发展，带来了更加广泛的应用．例如，FFT的提出，使得用DFT来计算两个长序列的卷积变得有实际意义了，而卷积运算在电子计算机科学和其他一些领域都有广泛的应用．

然而，在数字信号序列长度N很大的情况下，FFT的计算量仍嫌太大．于是人们努力寻求更快、更新的算法．

七十年代初，Rader，Agarwal，Burrus等人提出了构造整数模M剩余类环Z_M上的DFT，即数论变换，这种变换仍然具有循环卷积等特性，并可用类似FFT的快速演段来计算．这样，就可用数论变换来计算有理整数序列的卷积，与FFT比较，它具有更快的速度、没有舍入误差、不需要存贮三角函数等优点，其缺点是变换本身无物理意义（不能测量频率），以及序列长度要受运算字长的限制等．尽管如此，数论变换的提出，还是引起了人们的广泛注意，一方面是它的优点十分吸引人，更重要的一方面是数论变换把数论的方法带到了数字信号处理中，这从理论上和方法上讲，无疑是一个重要的进展．所以，自数论变换方法提出后，发展得很快，继之又提出了复数论变换和二次域上的某些变换等方法．

本书将系统介绍数论变换及其进一步推广的理论，以及这些理论所需要的数论基础知识．

应当指出，国外首先提出数论变换是重要的，其想法在数字信

号处理中也很有意义．但是，因为数论变换的理论还在发展，数论变换的应用也还处在探索阶段，所以国外关于这方面工作的研究还不完善．1976 年以来，我们在学习国外资料的基础上，开展了对数论变换的较系统的研究．本书也总结了我们自己在这方面的工作：

1. 利用我们给出的 Z_M 上 DFT 存在的一组充分必要条件，可以求出 Z_M 上 DFT 的个数，以及得到所有这些变换的算法，并简化了 Z_M 上 DFT 的定义．

2. 为了缩短字长和进行二维滤波，需要引入二维的数论变换．Z_M 上的二维 DFT，国外只给出了一组含混不清的充分条件，我们给出了充分必要条件，以及全部变换的个数和算法．用这个方法可立即得到一般 Z_M 上 m 维 $(m \geqslant 3)$ DFT 的相应的结果．而且，我们还简化了 Z_M 上的二维 DFT 的定义．并对序列长度和运算字长之间的关系，作了较细致的讨论．

3. 求复整数序列的卷积，就需要复数论变换．一般二次域 $R(\sqrt{m})$ 的整数剩余类环上 DFT 的构造问题，国外研究得很不充分，就是限定模 M 无平方因子的情况也未完全解决．而我们对任意的正整数 $M>1$，全部解决了 $R(\sqrt{m})$ 的模 M 整数剩余类环上的 DFT 的构造问题，包括 DFT 存在的充分必要条件，全部个数和算法．对于分圆域（包括实分圆域）上的情况，我们也解决了．

4. 熟知，在复数域上具有循环卷积性质的可逆变换存在而且是唯一的，即 DFT．但是在 Z_m 上如何呢？我们的工作揭示了这两种情况的本质差别．证明了在 Z_M 上存在非 DFT 型的有循环卷积性质的可逆变换（CRT）．而且，进一步给出了在任意有单位元素的交换环 R 上的 CRT 存在的充分必要条件和具体构造．同时还给出了二维的结果．

以上这些结果分别写进了第三章、第四章、第六章和第七章．此外从学习数论变换及其推广的需要出发，我们在第一章和第五章还分别介绍了初等数论和代数数论的基础知识．由于数论、代数、组合论等离散性数学已经深深地渗透到近代应用数学的各个

领域中，这些基础知识对于其他许多方面也是需要的.

通常把快速计算 DFT 的方法统称为快速变换. 作为计算方法的一个方面，其内容丰富，发展很快. 在第二章里我们除大致介绍一下 FFT 的实质外，还扼要介绍了某些新的快速变换，如素数幂变换和 WFTA 等. 第八章介绍了数论变换在其他方面的一些应用.

我们的工作始终是在柯召教授的热情指导下进行的. 在工作过程中还得到了中国科学院数学研究所、四机部 1014 所、四川大学无线电系等单位的有关同志的鼓励与支持，作者在此一并致以衷心地感谢.

限于水平，本书难免有缺点和错误，请读者批评指正.

作 者

一九七八年十二月

目　　录

第一章　初等数论………………………………………………… 1
§1. 整数的分解 ………………………………………………… 1
§2. 同余式 ……………………………………………………… 12
§3. 二次剩余 …………………………………………………… 26
第二章　卷积运算和快速变换………………………………… 45
§1. 卷积运算 …………………………………………………… 45
§2. DFT ………………………………………………………… 46
§3. FFT ………………………………………………………… 48
§4. 素数幂变换 ………………………………………………… 50
§5. WFTA ……………………………………………………… 55
第三章　数论变换的理论基础………………………………… 60
§1. 数论变换和快速数论变换 ………………………………… 60
§2. 数论变换的具体构造 ……………………………………… 63
§3. Fermat 数变换……………………………………………… 67
§4. 用快速数论变换计算循环卷积 …………………………… 68
§5. 三项式变换 ………………………………………………… 70
§6. 二维数论变换 ……………………………………………… 73
§7. 用二维快速数论变换计算一维卷积 ……………………… 77
§8. 多维数论变换 ……………………………………………… 84
§9. 用孙子定理减少字长 ……………………………………… 87
第四章　Fermat 数变换实现中的若干问题…………………… 89
§1. 流向图与蝶件 ……………………………………………… 89
§2. 计算机上模 F_t 运算的实现 ……………………………… 94
§3. 字长与序列长度间的关系 ………………………………… 106
§4. 用快速 Fermat 数变换与 FFT 计算卷积运算量的比较 ……… 111
第五章　代数数论初步………………………………………… 115
§1. 环和域 ……………………………………………………… 115

§2. 代数数和代数数域 …… 116
§3. $R(\theta)$ 的基底和整底 …… 123
§4. 整除性和素数 …… 128
§5. 理想数，同余 …… 129
§6. 二次域 $R(\sqrt{m})$ …… 135
§7. 属于不同域的理想数 …… 144
§8. 素理想数的一些性质 …… 146
§9. $[p]$ 的分解 …… 148
§10. 在分圆域上$[p]$的分解 …… 152
第六章 二次域和分圆域内的 DFT 构造 …… 160
§1. 计算复整数序列的卷积 …… 160
§2. 在二次域 $R(\sqrt{m})$ 里计算卷积 …… 165
§3. 在分圆域里计算卷积 …… 175
第七章 任意环上具有循环卷积性质的可逆变换 …… 181
§1. 引言 …… 181
§2. 任意环上的 CRT …… 181
§3. Z_M 上的 CRT …… 188
§4. 二维 CRT …… 194
第八章 数论变换在其他方面的应用 …… 199
§1. $GF(p^n)$上的多项式相乘 …… 199
§2. 大整数相乘 …… 200
§3. $F=GF(p)$ 上的多项式的除法 …… 200
§4. 计算序列的相关函数 …… 201
参考文献 …… 204

第一章　初等数论

§1. 整数的分解

数论是研究数的规律，特别是整数的规律的数学分支. 整除是数论中的基本概念，本节从这个概念出发，引进带余除法和辗转相除法，证明了数论中最基本的定理——唯一分解定理以及介绍这个定理的一些应用.

1.1. 整除性　我们知道两个整数的和、差、积仍然是整数，但是用一个不等于零的整数去除另一个整数所得的商却不一定是整数，因此，我们引进整除的概念.

定义. 设 a，b 是任意两个整数，其中 $b \neq 0$，如果存在一个整数 q 使得等式

$$a = bq \tag{1}$$

成立，我们就说 b 整除 a 或 a 被 b 整除，记作 $b|a$，此时我们把 b 叫作 a 的因数，把 a 叫作 b 的倍数.

如果(1)里的整数 q 不存在，我们就说 b 不能整除 a 或 a 不能被 b 整除，记作 $b \nmid a$.

由整除的定义出发，下面几个性质是明显的.

(i) 如果 $b|a$，$c|b$，则 $c|a$.

(ii) 如果 $b|a$，则 $cb|ca$.

(iii) 如果 $c|a$，$c|b$，则对任意的整数 m，n，有 $c|ma+nb$.

以上三条性质中，我们总假定，$b \neq 0$，$c \neq 0$.

在一般的情形下，有下面的定理.

定理 1. 设 a，b 是两个整数，其中 $b > 0$，则存在两个唯一的整数 q 及 r，使得

$$a = bq + r,\quad 0 \leqslant r < b \tag{2}$$

成立.

证. 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

则 a 必在上述序列的某两项之间,即存在一个整数 q 使得

$$qb \leqslant a < (q+1)b$$

成立. 令 $a - qb = r$, 则 (2) 成立.

设 q_1, r_1 是满足 (2) 的另一对整数,因为

$$bq_1 + r_1 = bq + r,$$

于是

$$b(q - q_1) = r_1 - r,$$

故

$$b|q - q_1| = |r_1 - r|.$$

由于 r 及 r_1 都是小于 b 的正整数, 所以上式右边是小于 b 的. 如果 $q \neq q_1$, 则上式左边 $\geqslant b$, 这是不可能的. 因此 $q = q_1$, $r = r_1$. 证完.

我们把 (2) 中的 q 叫做 a 被 b 所除得的不完全商, r 叫做 a 被 b 除所得到的余数,常记 $\langle a\rangle_b = r$.

1.2. 最大公因数与辗转相除法 我们用带余数除法, 研究整数的最大公因数的存在问题和实际求法.

定义. 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数. 若整数 d 是它们之中每一个的因数,那么 d 就叫作 $a_1, a_2, \cdots, a_n$ 的一个公因数. 整数 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个叫作最大公因数,记作 $(a_1, a_2, \cdots, a_n)$, 若 $(a_1, a_2, \cdots, a_n) = 1$, 我们说 $a_1, a_2, \cdots, a_n$ 互素. 我们有下面的定理.

定理 1. 设 a, b, c 是任意三个不全为零的整数, 且

$$a = bq + c,$$

其中 q 是整数,则 $(a, b) = (b, c)$.

证. 因为 $(a, b)|a$, $(a, b)|b$, 则有 $(a, b)|c$,因而 $(a, b) \leqslant (b, c)$, 同法可证 $(b, c) \leqslant (a, b)$, 于是得到 $(a, b) = (b, c)$. 证完.

因为显然有 $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$ 和

$b>0$, $(0, b)=b$, 所以下面我们只讨论两个正整数的最大公因数的求法,即辗转相除法,并借此推出最大公因数的若干性质.

设 a, b 是任意两个正整数,由带余除法,有下列等式:

$$\begin{aligned}
&a=bq_1+r_1, \quad 0<r_1<b,\\
&b=r_1q_2+r_2, \quad 0<r_2<r_1,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \qquad (1)\\
&r_{n-2}=r_{n-1}q_n+r_n, \quad 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, \quad r_{n+1}=0,
\end{aligned}$$

因为

$$b>r_1>r_2>r_3>\cdots\cdots,$$

故经有限次带余除法后,总可以得到一个余数是零,即 (1) 中 $r_{n+1}=0$.

现在我们证明定理 2.

定理 2. 若 a, b 是任意两个正整数,则 (a, b) 就是 (1) 中最后一个不等于零的余数,即 $(a, b)=r_n$.

证. 由定理 1 即得

$$\begin{aligned}
r_n&=(0, r_n)=(r_n, r_{n-1})=\cdots=(r_2, r_1)\\
&=(r_1, b)=(a, b), \quad \text{证完.}
\end{aligned}$$

我们从 (1) 中顺次由第一个等式解出 $r_1=a-bq_1$ 后代入第二个式子得 $r_2=-aq_2+b(1+q_1q_2)$, 再代入第三个式子解出 r_3, 然后代入第四个式子,这样作下去,最后可得

$$r_n=ma+nb,$$

这里的 m, n 是两个整数. 于是得到定理 3.

定理 3. 若 a, b 是任意两个正整数,则存在两个整数 m, n 使得

$$(a, b)=ma+nb.$$

定理 4. 若 $a\neq 0$, $a|bc$, $(a, b)=1$, 则 $a|c$.

证. 若 $c\neq 0$, 由 $(a, b)=1$ 知存在两个整数 m, n 使 $ma+nb=1$, 故 $mac+nbc=c$, 由 $a|bc$, 知 $a|c$, 若 $c=0$, 结论显然成立. 证完.

例. 求 323 和 221 的最大公因数.

$$
\begin{array}{r|l}
323 & 221 \\
221 & 1 \\
\hline
221 & 102 \\
204 & 2 \\
\hline
102 & 17 \\
102 & 6 \\
\hline
0 &
\end{array}
\qquad
\begin{array}{l}
323 = 221 \times 1 + 102, \\
221 = 102 \times 2 + 17, \\
102 = 17 \times 6, \\
\text{故 } (323, 221) = 17.
\end{array}
$$

再从第一个式子解出 102 代入第二个式子得

$$17 = (-2) \times 323 + 3 \times 221,$$

即得定理 3 中的 $m = -2$, $n = 3$.

现在来研究两个以上整数的最大公因数. 不妨假设 a_1, $a_2, \cdots, a_n$ 是任意 n 个正整数. 令

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \cdots, \quad (d_{n-1}, a_n) = d_n,$$

于是有下面的定理.

定理 5. 若 $a_1, a_2, \cdots, a_n$ 是 n 个正整数,则

$$(a_1, a_2, \cdots, a_n) = d_n.$$

证. 由 1.1. 节中的 (ii) 知,

$$d_n | a_n, \quad d_n | d_{n-1},$$

但

$$d_{n-1} | a_{n-1}, \quad d_{n-1} | d_{n-2},$$

故

$$d_n | a_{n-1}, \quad d_n | d_{n-2},$$

由此类推,最后得到

$$d_n | a_n, \quad d_n | a_{n-1}, \cdots, \quad d_n | a_1,$$

便有 $d_n \leqslant (a_1, a_2, \cdots, a_n)$, 另一方面,设 $(a_1, a_2, \cdots, a_n) = d$, 由 1.1. 节中的 (ii) 和定理 3 可得

$$d | d_2, \quad d | d_3, \cdots, \quad d | d_n,$$

故

$$d \leqslant d_n,$$

于是得到

$$(a_1, a_2, \cdots, a_n) = d_n.$$

证完.

1.3. 最小公倍数

定义. 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数 $(n \geqslant 2)$，若 m 是这 n 个数中每一个数的倍数，则 m 就叫作这 n 个数的一个公倍数. 在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中的最小正数叫作最小公倍数，记作 $[a_1, a_2, \cdots, a_n]$.

因为乘积 $a_1a_2\cdots a_n$ 就是 $a_1, a_2, \cdots, a_n$ 的一个公倍数，故最小公倍数是存在的.

由于任何正整数都不是零的倍数，故讨论整数的最小公倍数时，总假定这些整数都不是零.

和最大公因数一样，显然有 $[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|]$，所以只需对正整数讨论它们的最小公倍数.

我们先研究两个正整数的最小公倍数.

定理 1. 设 a, b 是任意两个正整数，则 (i) a, b 的所有公倍数就是 $[a, b]$ 的所有倍数；(ii) $[a, b] = \dfrac{ab}{(a, b)}$.

证. 设 m 是 a, b 的任一公倍数，$m = ak = bk'$，令

$$a = a_1(a, b) \quad 和 \quad b = b_1(a, b),$$

代入上式得 $$a_1k = b_1k',$$

由于 $$(a_1, b_1) = 1,$$

故 $$b_1 | k.$$

因此

$$m = ak = a(b, t) = \frac{ab}{(a, b)}t, \tag{1}$$

其中 t 满足等式 $k = b_1t$，反之，当 t 为任一整数时，$\dfrac{ab}{(a, b)}t$ 为 a, b 的一个公倍数，故 (1) 可以表示 a, b 的一切公倍数. 令 $t = 1$，即得最小的正数，故 $[a, b] = \dfrac{ab}{(a, b)}$. 即证明了 (ii)；又由 (1)，(i) 亦得证.

现在讨论两个以上整数的最小公倍数. 设 $a_1, a_2, \cdots, a_n$ 是 n 个正整数，令

$$[a_1, a_2] = m_2, \quad [m_2, a_3] = m_3, \cdots, [m_{n-1}, a_n] = m_n, \quad (2)$$

我们有定理 2.

定理 2. 若 $a_1, a_2, \cdots, a_n$ 是 $n(n \geqslant 2)$ 个正整数，则

$$[a_1, a_2, \cdots, a_n] = m_n.$$

证. 由 (2) 知，$m_i | m_{i+1}$，$i = 2, 3, \cdots, n-1$，且 $a_1 | m_2$，$a_i | m_i$，$i = 2, \cdots, n$，故 m_n 是 $a_1, a_2, \cdots, a_n$ 的一公倍数，又设 m 是 $a_1, a_2, \cdots, a_n$ 的任一公倍数，则 $a_1 | m$，$a_2 | m$，故由定理 1 的(i)，$m_2 | m$. 又 $a_3 | m$，同理可得 $m_3 | m$，依此类推，最后得 $m_n | m$. 因此 $m_n \leqslant |m|$. 故

$$m_n = [a_1, a_2, \cdots, a_n].$$

我们已经讲了最大公因数的求法，因此上面两个定理给出了最小公倍数的求法.

1.4. 素数，唯一分解定理 在正整数里，1 的因数就只有它本身. 任一个大于 1 的整数都至少有两个正因数，即 1 和它本身.

定义. 一个大于 1 的整数，如果它的正因数只有 1 和它本身，就叫作素数，否则就叫作复合数.

本节的主要目的就是要证明任何一个大于 1 的整数，如果不论次序，能唯一地表示成素数的乘积.

定理 1. 设 a 是任一大于 1 的整数，则 a 的除 1 以外的最小正因数 q 是素数，并且当 a 是复合数时，$q \leqslant \sqrt{a}$.

证. 假定 q 不是素数，由定义，q 除 1 和它本身外还有一正因数 q_1，因而 $1 < q_1 < q$，但 $q | a$，所以 $q_1 | a$，这与 q 是最小正因数矛盾，故 q 是素数.

当 a 是复合数时，则 $a = a_1 q$，且 $q \leqslant a_1$，故 $q \leqslant \sqrt{a}$. 证完.

定理 2. 若 p 是一素数，a 是任一整数，则有 $p | a$ 或 $(p, a) = 1$.

证. 因为 $(p, a) | p$，故 $(p, a) = 1$ 或 $(p, a) = p$. 即 $(p, a) = 1$ 或 $p | a$. 证完.

定理 3. 若 p 是素数，$p|ab$，则 $p|a$ 或 $p|b$.

证. 若 $p\nmid a$，则由定理 2 知 $(p, a)=1$，由 §1.2 定理 4 知 $p|b$. 证完.

定理 4（唯一分解定理）. 任一大于 1 的整数能表示成素数的乘积，即整数 $a>1$，

$$a=p_1p_2\cdots p_n, \quad p_1\leqslant p_2\leqslant\cdots\leqslant p_n, \tag{1}$$

其中 $p_1, p_2, \cdots, p_n$ 是素数，并且若

$$a=q_1q_2\cdots q_m, \quad q_1\leqslant q_2\leqslant\cdots\leqslant q_m, \tag{2}$$

其中 $q_1, q_2, \cdots, q_m$ 是素数，则 $m=n$，$q_i=p_i$ $(i=1, 2, \cdots, n)$.

证. 我们用数学归纳法首先证明 (1) 式成立，当 $a=2$ 时(1)式显然成立. 假定对于一切小于 a 的正整数 (1) 式都成立，此时若 a 是素数，则 (1) 式对 a 成立，若 a 是复合数，则有两个正整数 b，c 满足条件

$$a=bc, \quad 1<b\leqslant c<a.$$

由假定 b 和 c 分别能表示成素数的乘积，故 a 能表成素数的乘积，即 (1) 式成立. 由归纳法即知对任一大于 1 的正整数，(1) 式成立. 若对 a 同时有 (1)，(2) 两式成立，则

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m. \tag{3}$$

由定理 3 知有 p_k，q_j 使得 $p_1|q_j$，$q_1|p_k$，但 q_j，p_k 都是素数，所以 $p_1=q_j$，$q_1=p_k$，又 $p_k\geqslant p_1$，$q_j\geqslant q_1$，故同时有 $p_1\geqslant q_1$ 和 $q_1\geqslant p_1$，因而 $p_1=q_1$，由(3)式得 $p_2\cdots p_n=q_2\cdots q_m$. 同理可得 $p_2=q_2$，$p_3=q_3$. 依此类推，最后得 $m=n$. 证完.

这个定理告诉我们，任一大于 1 的正整数 a 能够唯一地写成

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}, \quad \alpha_i>0 \quad (i=1, 2, \cdots, k), \tag{4}$$

其中 $p_i<p_j$，$(i<j)$ 是素数.

(4) 叫做 a 的标准分解式.

于是，当 $d|a$，$d>0$，由 (4) d 可以表示成

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}, \quad \alpha_i\geqslant\beta_i\geqslant 0 \quad (i=1, 2, \cdots, k) \tag{5}$$

的形式，反之 d 可以表示成 (5) 的形式时，一定有 $d|a$，$d>0$.

作为唯一分解定理的一个简单而直接的应用，我们有：

设 a, b 是任意两个正整数，且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0 \quad (i = 1, 2, \cdots, k),$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad \beta_i \geqslant 0 \quad (i = 1, 2, \cdots, k),$$

则

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \quad \gamma_i = \min(\alpha_i, \beta_i) \quad (i = 1, \cdots, k),$$
$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \quad \delta_i = \max(\alpha_i, \beta_i) \quad (i = 1, \cdots, k),$$

符号 $\min(\alpha_i, \beta_i)$ 表示 α_i, β_i 中较小的数，$\max(\alpha_i, \beta_i)$ 表示 α_i, β_i 中较大的数.

对于任意整数 x, y 显然有

$$x + y = \max(x, y) + \min(x, y).$$

由此，我们又可得出 § 1.3 定理 1 的结果：

$$[a, b] = \frac{ab}{(a, b)}.$$

上面从理论上证明了任意一个大于 1 的正整数有唯一的标准分解，但在实际计算中，还没有一个简单而有效的方法去判断哪些正整数是素数，也没有一个简单而有效的方法求出一个正整数的标准分解式. 但另一方面，我们根据素数的定义及其性质，可以造出素数表来以供使用.

任给一个正整数 N，可以按照下述方法求出一切不超过 N 的素数，把不超过 N 的一切正整数按大小顺序排成一串

$$1, 2, 3, 4, \cdots, N,$$

首先划去 1，第一个留下的是 2，它是一个素数：

$$\not{1}, 2, 3, 4, \cdots, N,$$

其次从 2 起，划出除 2 以外的 2 的一切倍数，

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, \cdots, N,$$

在 2 的后面第一个未划去的是 3，它不是 2 的倍数，因此是一个素数. 然后划去的数是 $3m$ $(m = 2, 3, \cdots)$，

~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, $\cdots$, N ,

紧接着 3 后面未划去的是 5，它不是比它小的那些素数(2 及 3)的倍数，因此它是素数．然后划去的数是 $5m$ $(m=2,3,\cdots)$，

~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, $\cdots$, N,

如此继续下去，所划去的数都是复合数，每次划后第一个留下的数都不是比它小的素数的倍数，因此总是素数．用这种方法可以逐一地把素数求出来，这个方法叫筛法．

要求出不超过 N 的一切素数，根据定理 1，只需把不超过 $\sqrt{N}$ 的素数的倍数划去就行了．因为不超过 N 的复合数的最小素因数总是不超过 $\sqrt{N}$ 的．

为了更清楚地了解素数表的造法，我们举 $N=30$ 为例．此时 $\sqrt{30}<6$．故只需在下表中划去 1 与 2，3，5 的倍数就行了

~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~,
17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~,

所以不超过 30 的素数是 2，3，5，7，11，13，17，19，23，29．

上述造素数表的方法并不能在有限步骤以内把正整数中的一切素数都找出来，因为我们有下述定理．

定理 5． 素数的个数是无穷的．

证．我们用反证法来证明定理．假定正整数中只有有限个素数，设为 $p_1, p_2, \cdots, p_k$，令 $p_1p_2\cdots p_k+1=N$，则 $N>1$，由定理 1 知 N 有一个素因数 p，这里 $p\neq p_i$ $(i=1,2,\cdots,k)$，否则，$p/p_1p_2\cdots p_k$，p/N，推出 $p/1$，与 p 是素数矛盾．故 p 是上面 k 个素数以外的素数．证完．

1.5. $n!$ 中素因数的方次 在这里，我们将求出 $n!$ 的标准分解式．为此，我们先介绍数论中常常用到的函数 $[x]$．

定义． 函数 $[x]$ 是对于一切实数都有定义的函数，函数 $[x]$ 的值等于不大于 x 的最大整数．

例. $[\pi]=3$, $[-\pi]=-4$, $\left[\frac{2}{3}\right]=0$, $\left[-\frac{4}{7}\right]=-1$.

由定义可立刻得出下列简单性质:

1° $[x]\leqslant x<[x]+1$.

2° $[x]+[y]\leqslant[x+y]$.

3° $[n+x]=n+[x]$, n 是整数.

4° $[-x]=\begin{cases}-[x]-1, & \text{当 } x \text{ 不是整数,}\\ -[x], & \text{当 } x \text{ 是整数.}\end{cases}$

5° 若 a, b 是任意两个正整数,则不大于 a 而为 b 的倍数的正整数个数是 $\left[\frac{a}{b}\right]$.

证. $a<b$ 时显然, 设 m 是任一不大于 a 而为 b 的倍数的正整数,则

$$0<m=bm_1\leqslant a,$$

$$0<m_1\leqslant\frac{a}{b}. \tag{1}$$

故满足以上条件的 m 的个数等于满足 (1) 的 m_1 的个数,因而等于 $\left[\frac{a}{b}\right]$, 证完.

定理 1. 在 $n!$ 的标准分解式中素因数 $p(p\leqslant n)$ 的方幂数 h 为

$$h=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right], \tag{2}$$

注意, 当 $p^s>n$ 时 $\left[\frac{n}{p^i}\right]=0, i=s, s+1,\cdots$, 因而(2)式有意义.

证. 设想把 $2, 3, \cdots, n$ 都分解成标准分解式,则由唯一分解定理可知, h 就是这 $n-1$ 个分解式中 p 的方幂数之和. 设其中 p 的方幂数是 r 的有 n_r 个 $(p\geqslant 1)$, 则

$$\begin{aligned}h&=n_1+2n_2+3n_3+\cdots\\&=n_1+n_2+n_3+\cdots\end{aligned}$$

$$
\begin{aligned}
&+ n_2 + n_3 + \cdots \\
&\qquad + n_3 + \cdots \\
&\qquad\qquad + \cdots \\
&= N_1 + N_2 + N_3 + \cdots,
\end{aligned}
$$

其中 $N_r = n_r + n_{r+1} + \cdots$ 恰好是 $n-1$ 个数 $2,\cdots,n$ 中能被 p^r 整除的个数，由性质 5，$N_r = \left[\dfrac{n}{p^r}\right]$，故

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right].$$ 证完.

这个定理给出了 $n!$ 的标准分解式

$$n! = \prod_{p \leqslant n} p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]},$$

其中 $\prod\limits_{p \leqslant n}$ 表示展布在不超过 n 的一切素数上的积式.

定理 2. $\dfrac{n!}{k!(n-k)!}$ 是整数 $(0 < k < n)$.

证. 由性质 3 及 $n = (n-k) + k$,

$$\left[\frac{n}{p^r}\right] \geqslant \left[\frac{n-k}{p^r}\right] + \left[\frac{k}{p^r}\right],$$

$$\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right] \geqslant \sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right],$$

故

$$\prod_{p \leqslant n} p^{\sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right]} \Bigg| \prod_{p \leqslant n} p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]},$$

即 $k!(n-k)! \mid n!$. 证完.

1.6. 一次不定方程 不定方程是指未知数的个数多于方程的个数，而且未知数须受某种限制（如整数，正整数或有理数等）的方程. 本小节给出二元一次方程的解法.

定理 1. 设 a, b, c 是给定的整数，$ab \neq 0$，则方程

$$ax + by = c \tag{1}$$

有整数解 x, y 的充分必要条件是 $(a, b)|c$.

证. 必要性是明显的. 反之, 若 $(a, b)|c$ 则 $c=c_1(a, b)$, c_1 是整数. 由 § 1.2 定理 3 知, 存在两个整数 m, n 满足等式 $am+bn=(a,b)$, 令 $x_0=mc_1$, $y_0=nc_1$, 即得

$$ax_0+by_0=c,$$

故 (1) 有整数解 x_0, y_0. 证完.

这个定理告诉我们, 当 (1) 有整数解时, 如何求出 (1) 的一组解来. 然而, 知道了一组解, 如何求出 (1) 的全部解呢? 我们有定理 2.

定理 2. 设 (1) 有一组解 x_0, y_0, 又 $(a, b)=d$, $a=a_1d$, $b=b_1d$, 则 (1) 的一切整数解可以表示成

$$x=x_0-b_1t, \quad y=y_0+a_1t, \quad t=0, \pm 1, \cdots. \tag{2}$$

证. 将 (2) 代入 (1) 得

$$a(x_0-b_1t)+b(y_0+a_1t)=c+(ba_1-ab_1)t=c,$$

这表明 (2) 是 (1) 的解.

设 x_1, y_1 是 (1) 的任一解, 则 $ax_1+by_1=c$, 由此式减去 $ax_0+by_0=c$, 即得

$$a(x_1-x_0)+b(y_1-y_0)=0.$$

由上式及 $a=a_1d$, $b=b_1d$ 得到

$$a_1(x_1-x_0)=-b_1(y_1-y_0). \tag{3}$$

由于 $(a_1,b_1)=1$, 故 $a_1|y_1-y_0$, 可能 $y_1-y_0=a_1t$, 亦即 $y_1=y_0+a_1t$, 将 y_1 代入 (3) 式即得 $x_1=x_0-b_1t$, 因此 x_1, y_1 可表示成 (2) 的形状. 故 (2) 表示 (1) 的一切整数解. 证完.

§ 2. 同 余 式

同余是数论中一个基本概念, 它所包含的内容较丰富, 应用也较广. 本节介绍同余的基本性质以及解某些同余式的一般方法.

2.1. 同余的概念 有时, 我们所要注意的常常不是某些整数, 而是这些数用某一固定的正整数去除所得的余数. 例如, 这个月

的3号是星期一，那么这个月的10号、17号、24号都是星期一，因为这些数用7去除都余3，这就是同余的例子．一般的，我们可以给出下面的定义．

定义．给定一个正整数 m，如果用 m 去除任意两个整数 a 与 b 所得的余数相同．我们就说 a，b 对模 m 同余、记作 $a \equiv b \pmod m$；如果余数不同，我们就说 a，b 对模 m 不同余，记作 $a \not\equiv b \pmod m$．

由定义立刻可得下列三个性质：

1° $a \equiv a \pmod m$．

2° $a \equiv b \pmod m$，则 $b \equiv a \pmod m$．

3° $a \equiv b \pmod m$，$b \equiv c \pmod m$，则 $a \equiv c \pmod m$．

定理1．整数 a，b 对模 m 同余的充分必要条件是 $m \mid a - b$，即 $a = b + mt$，t 是整数．

证．设 $a = mq_1 + r_1$，$b = mq_2 + r_2$，$0 \leqslant r_1 < m$，$0 \leqslant r_2 < m$．若 $a \equiv b \pmod m$，则 $r_1 = r_2$，因此 $a - b = m(q_1 - q_2)$，反之若 $m \mid a - b$，则 $m \mid m(q_1 - q_2) + (r_1 - r_2)$，因此 $m \mid r_1 - r_2$，但 $|r_1 - r_2| < m$．故 $r_1 = r_2$．证完．

这个定理说明同余这一概念又可定义如下：若 $m \mid a - b$，则 a，b 叫做对模 m 同余．

由定理1及整除的性质可以很容易得到下列性质：

4° 若 $a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，则

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m.$$

5° 若 $a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，则

$$a_1 a_2 \equiv b_1 b_2 \pmod m.$$

这两个性质与等式类似，但也有不相同的．如从同余式来讲，由 $a \not\equiv 0 \pmod m$ 和 $aa_1 \equiv ab_1 \pmod m$，一般是不能得出 $a_1 \equiv b_1 \pmod m$ 的，$2 \equiv 2 \pmod 4$，$2 \cdot 3 \equiv 2 \cdot 1 \pmod 4$，但 $3 \not\equiv 1 \pmod 4$，就是例子．但有

6° 若 $ac \equiv bd \pmod m$，$c \equiv d \pmod m$ 及 $(c, m) = 1$，则

$$a \equiv b \pmod m.$$

证. 由 $(a-b)c+b(c-d)=ac-bd\equiv 0 \pmod{m}$, 可得 $m|(a-b)c$, 但 $(m,c)=1$, 故得 $m|a-b$. 证完.

2.2. 剩余类和完全剩余系 有了同余的概念，我们就可以把余数相同的数放在一起，这样就产生了剩余类的概念.

上节中，同余的性质 1 叫反身性，性质 2 叫对称性，性质 3 叫递推性. 这样对给定的任一正整数 m，利用模 m 同余这个关系，就可以将全部整数分成若干类. 我们有

定理 1. 若 m 是一个给定的正整数，则全部整数可以分成 m 个集合，记作 $C_0, C_1, \cdots, C_{m-1}$，其中 $C_r(r=0,1,\cdots,m-1)$ 是由一切形如 $qm+r(q=0,\pm 1,\pm 2,\cdots)$ 的整数所组成的. 这些集合具有下列性质:

1° 每一整数必包含在而且仅在上述的一个集合里面.

2° 两个整数同在一个集合的充分必要条件是这两个整数对模 m 同余.

证. (i) 设 a 是任一整数，由 § 1.1 定理 1 即得

$$a=a_1m+r_a, \quad 0\leqslant r_a<m,$$

故 a 在 C_{r_a} 内. 又 r_a 是由 a 唯一确定的，因此 a 只能在 C_{r_a} 内.

(ii) 设 a, b 是两个整数，并且都在 C_r 内，则

$$a=q_1m+r, \quad b=q_2m+r,$$

故 $a\equiv b \pmod{m}$. 反之若 $a\equiv b \pmod{m}$，则由同余的定义即知 a 和 b 同在某一 C_r 内. 证完.

现在我们讨论的对象是整数，数学讨论的对象还有很多，如代数中的实数，复数，几何中的点，直线，三角形等等，我们把讨论的对象取个名，统统叫元素. 所谓集合就是指若干个(有限或无限多个)元素的全体，以后我们把集合简称为集. 由定理 1 得到的用同余对整数集合分类的结果，对一般集也是对的，即是说；设集 M 中的元素间可以建立一个满足反身性，对称性，递推性的关系(叫等价关系)，所有与一个元素等价的元素的集叫做一类，那么 M 中的元素就能够分成若干没有公共元素的类而无遗漏.

把集分类加以讨论，有助于对集的认识.

定义. 定理 1 中的 $C_0, C_1, \cdots, C_{m-1}$ 叫做模 m 的剩余类. 在模 m 的剩余类中任取一数作为该类的代表，此 m 个数称为模 m 的完全剩余系.

由定理 1 和上述定义，立刻得到下面的定理.

定理 2. m 个整数作成模 m 的一个完全剩余系的充分必要条件是两两对模 m 不同余.

最常用的完全剩余系是 $0, 1, 2, \cdots, m-1$，它们称为模 m 的非负最小完全剩余系.

定理 3. 若 m_1, m_2 是互素的两个正整数，而 x_1, x_2 分别通过模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 通过模 m_1m_2 的完全剩余系.

证. 由假设知道 x_1, x_2 分别通过 m_1, m_2 个整数，因此 $m_2x_1 + m_1x_2$ 通过 m_1m_2 个整数. 由定理 2 只需证明这 m_1m_2 个整数对模 m_1m_2 两两不同余就够了. 假定

$$m_2x_1' + m_1x_2' \equiv m_2x_1'' + m_1x_2'' \pmod{m_1m_2}, \tag{1}$$

其中 x_1', x_1'' 是 x_1 所通过的完全剩余系中的整数，而 x_2', x_2'' 是 x_2 所通过的完全剩余系中的整数，则由同余式性质即得

$$m_2x_1' \equiv m_2x_1'' \pmod{m_1}, \quad m_1x_2' \equiv m_1x_2'' \pmod{m_2}.$$

由 $(m_1, m_2) = 1$，用 § 2.1 中性质 6 即得 $x_1' \equiv x_1'' \pmod{m_1}$，$x_2' \equiv x_2'' \pmod{m_2}$，但 x_1', x_1'' 是模 m_1 的完全剩余系中的两个数，故 $x_1' = x_1''$，同样 $x_2' = x_2''$，这表明如果 x_1', x_2' 与 x_1'', x_2'' 不全相同，则 (1) 式不能成立. 证完.

顺便指出，模 m 的剩余类之间可以定义运算. 由 § 2.1 的性质 4 及 5 知道，在任给的两个剩余类 A 和 B 中各取一代表 a 和 b，而令 $a + b$(或 $a \cdot b$)所在的剩余类为 C，则 C 仅与 A, B 有关，而与所选之代表 a, b 无关，故可定义剩余类 C 为剩余类 A, B 之和(或积). 这里，我们给出了元素不是数而是剩余类之间的运算的例子. 更一般的情形，我们将在下一节里讨论.

2.3. 缩系和数论函数 $\varphi(n)$ 这里，讨论完全剩余系中与模互素的整数，先引进缩系的概念. 在讨论缩系的过程中，需要引入一

个常用的数论函数——Euler 函数 $\varphi(n)$. 我们有

定义. Euler 函数 $\varphi(n)$ 是一个数论函数，它在正整数 n 上的值等于序列 $0, 1, 2, \cdots, n-1$ 中与 n 互素的数的个数.

由定义知 $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2, \cdots$, 当 p 是素数时,有 $\varphi(p)=p-1$.

定义. 如果一个模 m 的剩余类里面的数与 m 互素(显然,只要有一个与 m 互素,其余的均与 m 互素)，就把它叫做一个与模 m 互素的剩余类. 在与模 m 互素的全部剩余类中，各任取一数所组成的集叫做缩系.

显然有:

定理 1. 与模 m 互素的剩余类的个数是 $\varphi(m)$.

定理 2. 若 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数，则 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是模 m 的一个缩系的充分必要条件是它们两两对模 m 不同余.

定理 3. 若 $(a, m)=1$, x 通过模 m 的缩系,则 ax 也通过模 m 的缩系.

证. ax 通过 $\varphi(m)$ 个整数，由于 $(a, m)=1$, $(x, m)=1$, 故 $(ax, m)=1$, 若 $ax_1 \equiv ax_2 \pmod{m}$, 可得 $x_1 \equiv x_2 \pmod{m}$, 这与原假设矛盾,故由定理 2，定理得证.

定理 4. 设 m 是大于 1 的整数，$(a, m)=1$, 则

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

证. 设 $r_1, r_2, \cdots, r_{\varphi(m)}$ 是模 m 的缩系，则由定理 3 $ar_1, ar_2, \cdots, ar_{\varphi(m)}$ 也是模 m 的缩系,故

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

即

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

由

$$(r_i, m)=1, \quad i=1, 2, \cdots, \varphi(m)$$

得

$$(r_1 r_2 \cdots r_{\varphi(m)}, m)=1,$$

故有

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

证完.

由定理 4 立刻推出定理 5.

定理 5. 若 p 是素数,则

$$a^p \equiv a \pmod p.$$

2.4. $\varphi(m)$ 的积性 本小节给出计算 $\varphi(n)$ 值的公式.

定理 1. 若 m_1, m_2 是两个互素的正整数, x_1, x_2 分别通过模 m_1, m_2 的缩系,则 $m_2x_1 + m_1x_2$ 通过模 m_1m_2 的缩系.

证. (i) 若 $(x_1, m_1) = 1$, $(x_2, m_2) = 1$, 则由 $(m_1, m_2)=1$ 得 $(m_2x_1, m_1) = (m_1x_2, m_2) = 1$, 所以 $(m_2x_1 + m_1x_2, m_1) = (m_2x_1 + m_1x_2, m_2) = 1$, 故 $(m_2x_1 + m_1x_2, m_1m_2) = 1$.

(ii) 反之,凡与 m_1m_2 互素之 a 必与 $m_2x_1 + m_1x_2$ 中之一同余. § 2.2 定理 3 告诉我们对任一整数 a 必有 x_1, x_2 使

$$a \equiv m_2x_1 + m_1x_2 \pmod{m_1m_2},$$

所以只需说明当 $(a, m_1m_2) = 1$ 时, $(x_1, m_1) = (x_2, m_2) = 1$ 就够了. 今若 $(x_1, m_1) = d > 1$, 则 $(a, m_1) = (m_2x_1 + m_1x_2, m_1) = (m_2x_1, m_1) = (x_1, m_1) = d$, 此与 $(a, m_1m_2) = 1$ 矛盾. 同样可证 $(x_2, m_2) = 1$.

(iii) 由 § 2.2 定理 3 知 $m_2x_1 + m_1x_2$ 中任两个对模 m_1m_2 均不同余.

综上所述,定理得证.

由这一定理即可推出下面两个定理.

定理 2. 若 $(m_1, m_2) = 1$, 则 $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$.

定理 3. 设 n 的标准分解式为 $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, 则

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \quad (1)$$

证. (i) 由定理 2 即得

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k}).$$

(ii) 今证明 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. 由 $\varphi(n)$ 的定义知 $\varphi(p^\alpha)$ 等于从 p^α 减去 $1, \cdots, p^\alpha$ 中与 p^α 不互素(即与 p 不互素)的

数的个数．由于 p 是素数，故 $\varphi(p^\alpha)$ 等于从 p^α 减去 $1,\cdots,p^\alpha$ 中被 p 整除的数的个数，由第二章 § 1.5 的性质 5 知这个数是

$$\left[\frac{p^\alpha}{p}\right] = p^{\alpha-1},$$

故

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

(iii) 由 (i), (ii) 即得

$$\begin{aligned}\varphi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$ 证完．

2.5. 一次同余式 代数的一个主要问题是解方程，这里讨论类似的问题．求同余式的解．本节讨论一次同余式．先给出一般的概念．

定义． 若用 $f(x)$ 表示多项式 $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$，其中 a_i 是整数，又设 m 是一个正整数，则

$$f(x) \equiv 0 \pmod m \tag{1}$$

叫模 m 的同余式．若 $a_n \not\equiv 0 \pmod m$，则 n 叫做 (1) 的次数．

显然，若 $f(a) \equiv 0 \pmod m$，则与 a 在同一剩余类中的任何数 a' 都能使 $f(a') \equiv 0 \pmod m$，因此有

定义． 若 a 是使 $f(a) \equiv 0 \pmod m$ 成立的一个整数，则 $x \equiv a \pmod m$ 叫做 (1) 的一个解．这就是说今后我们把适合 (1) 式而对模 m 相互同余的一切数算作 (1) 的一个解．

定理 1． 一次同余式

$$ax \equiv b \pmod m, \qquad a \not\equiv 0 \pmod m \tag{2}$$

有解的充分必要条件是 $(a,m)|b$．若 (2) 有解，则 (2) 的解数是 $d=(a,m)$．

证．容易看出 (2) 有解的充分必要条件是 $ax - my = b$ 有解，即知 (2) 有解的充分必要条件是 $(a,m)|b$．

设 $d=(a,m)$，若(2)有解，即 $ax - my = b$ 有解，由 § 1.6 定理 2 知，它的一切整数解可以表示成

$$x = m_1 t + x_0, \quad m_1 = \frac{m}{d} \quad (t = 0, \pm 1, \cdots),$$

此式对模 m 来说，可以写成

$$x \equiv x_0 + k m_1 \pmod{m} \quad (k = 0, 1, \cdots, d-1), \qquad (3)$$

但 $x_0 + k m_1$, $k = 0, 1, \cdots, d-1$ 是对模 m 两两不同余的，故 (2) 有 d 个解，即 (3). 证完.

由定理的证明可以看出，适合(2)的整数也就是适合不定方程 $ax - my = b$ 的解答中 x 的值，故同余式 (2) 可以用解上述不定方程的方法去解它.

2.6. 孙子定理 本节解同余式组

$$x \equiv b_1 \pmod{m_1}, \ x \equiv b_2 \pmod{m_2}, \cdots, \ x \equiv b_k \pmod{m_k}, \quad (1)$$

在我国古代孙子算经里已经提出了这种形式的问题，并且很好地解决了它. 孙子算经里所提出的问题之一如下:

"今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?"，这就是求一次同余式组:

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

的公解 x.

把孙子所用算法推广就成为定理 1.

定理 1（**孙子定理**）. 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, $m = m_i M_i$ $(i = 1, 2, \cdots, k)$, 则同余式组 (1) 的解是

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod{m}, \qquad (2)$$

其中

$$M_i' M_i \equiv 1 \pmod{m_i} \quad (i = 1, 2, \cdots, k).$$

证. 由 $(m_i, m_j) = 1$, $i \neq j$, 即得 $(M_i, m_i) = 1$, 由前节定理 1 知对每一 M_i, 有一 M_i' 存在, 使得 $M_i' M_i \equiv 1 \pmod{m_i}$, 另一方面由 $m = m_i M_i$, 因此 $m_j | M_i$, $i \neq j$, 故

$$\sum_{j=1}^{k} M_j' M_j b_j \equiv M_i' M_i b_i \equiv b_i \pmod{m_i},$$

即 (2) 为 (1) 的解.

若 x_1, x_2 是适合 (1) 式的任意两个整数，则

$$x_1 \equiv x_2 \pmod{m_i} \quad (i = 1, 2, \cdots, k),$$

因 $(m_i, m_j) = 1$，$i \neq j$，于是 $x_1 \equiv x_2 \pmod{m}$，故 (1) 式的解只有 (2)．证完．

在 $k = 2$ 时的一般情况，我们有定理2．

定理 2．一次同余式组

$$x \equiv b_1 \pmod{m_1}, \qquad x \equiv b_2 \pmod{m_2} \tag{3}$$

可解的充分必要条件是 $(m_1, m_2) | b_1 - b_2$，且当它可解时对模 $[m_1, m_2]$ 有唯一解．

证．设 (3) 有公解 x_0，记 $(m_1, m_2) = d$，则有

$$x_0 \equiv b_1 \pmod{d}, \qquad x_0 \equiv b_2 \pmod{d},$$

两式相减即得 $d | b_1 - b_2$．

反之，若 $(m_1, m_2) | b_1 - b_2$，则因 $x \equiv b_1 \pmod{m_1}$ 的一般解是 $x = b_1 + m_1 y$，代入 $x \equiv b_2 \pmod{m_2}$ 得

$$m_1 y \equiv b_2 - b_1 \pmod{m_2},$$

因 $(m_1, m_2) = d | b_2 - b_1$，故上式模 m_2 有解 y_0，且其全部解为

$$y = y_0 + \frac{m_2}{d} k \qquad (k = 0, \pm 1, \cdots),$$

故 (3) 之全部解为

$$x = b_1 + m_1 y_0 + \frac{m_1 m_2}{d} k \qquad (k = 0, \pm 1, \cdots),$$

这些解对模 $\frac{m_1 m_2}{d} = [m_1, m_2]$ 来说都是同余的．证完．

对于 $k \geqslant 3$，我们可先解第一、第二个同余式组，得到 $x \equiv b_2' \pmod{[m_1, m_2]}$ 再与 $x \equiv b_3 \pmod{m_3}$ 联立解出 $x \equiv b_3' \pmod{[m_1, m_2, m_3]}$，如此继续下去，最后可得(1)的唯一解 $x \equiv b_k' \pmod{[m_1, m_2, \cdots, m_k]}$．如果中间有一步无解，则 (1) 无解．

作为一个例子，我们用孙子定理解出

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}$$

应用孙子定理，取 $m_1 = 3$，$m_2 = 5$，$m_3 = 7$，则 $M_1 = 5 \cdot 7 =$

35, $M_2=3\cdot7=21$, $M_3=3\cdot5=15$, 而 M_1', M_2', M_3' 分别满足
$35M_1'\equiv1\pmod 3$, $21M_2'\equiv1\pmod 5$, $15M_3'\equiv1\pmod 7$,
即 $2M_1'\equiv1\pmod 3$, $M_2'\equiv1\pmod 5$, $M_3'\equiv1\pmod 7$, 取
$M_1'=2$, $M_2'=1$, $M_3'=1$, 于是

$$x\equiv\sum_{i=1}^{3}M_iM_i'b_i=70\cdot2+21\cdot3+15\cdot2\equiv23\pmod{3\cdot5\cdot7}.$$

最后,我们有定理 3.

定理 3. 设 $m_1, m_2, \cdots, m_k$ 两两互素,若 $b_1, b_2, \cdots, b_k$ 分别过 $m_1, m_2, \cdots, m_k$ 的完全剩余系,则(2)过模 $m=m_1m_2\cdots m_k$ 的完全剩余系

证. 令 $x_0=\sum_{i=1}^{k}M_i'M_ib_i$, 则 x_0 过 m 个数. 这 m 个数是两两不同余的,因为若

$$\sum_{i=1}^{k}M_i'M_ib_i'\equiv\sum_{i=1}^{k}M_i'M_ib_i''\pmod m,$$

则

$$M_i'M_ib_i'\equiv M_i'M_ib_i''\pmod{m_i}\quad(i=1,2,\cdots,k),$$

故 $b_i'\equiv b_i''\pmod{m_i}$ $(i=1,2,\cdots,k)$, 这与假设矛盾. 所以由 §2.2 定理 2 即得定理的结论.

2.7. 高次同余式的解数及解法 本节初步地讨论一下高次同余式的求解. 我们的方法是先把复合数模的同余式化成素数幂模的同余式,然后讨论素数幂模的同余式的解法.

定理 1. 若 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数, $m=m_1m_2\cdots m_k$, 则同余式

$$f(x)\equiv0\pmod m \tag{1}$$

与同余式组

$$f(x)\equiv0\pmod{m_i}\quad(i=1,2,\cdots,k) \tag{2}$$

等价(即任一适合(1)的整数适合(2),反之任一适合(2)的整数亦适合(1)). 并且若用 T_i 表示 $f(x)\equiv0\pmod{m_i}$, $i=1,2,\cdots,k$

对模 m_i 的解数，T 表示 (1) 对模 m 的解数，则 $T = T_1T_2\cdots T_k$.

证. (i) 我们先证 (1) 和 (2) 等价. 设 x_0 是适合 (1) 的整数，则

$$f(x_0) \equiv 0 \pmod{m}$$

由 $m = m_1m_2\cdots m_k$，立即有

$$f(x_0) \equiv 0 \pmod{m_i} \qquad (i = 1, 2, \cdots, k),$$

反之，若 x_0 适合 (2)，则

$$f(x_0) \equiv 0 \pmod{m_i} \qquad (i = 1, 2, \cdots, k).$$

由 $(m_i, m_j) = 1$ $(i \neq j)$，故得

$$f(x_0) \equiv 0 \pmod{m_1m_2\cdots m_k}. \tag{3}$$

于是证明了 (1), (2) 等价.

(ii) 设 $f(x) \equiv 0 \pmod{m_i}$ 的 T_i 个不同的解是

$$x \equiv b_{i_{t_i}} \pmod{m_i} \quad (t_i = 1, 2, \cdots, T_i),$$

则 (2) 的解即下列诸同余式组

$$x \equiv b_{1t_1} \pmod{m_1},\ x \equiv b_{2t_2} \pmod{m_2}, \cdots,\ x \equiv b_{kt_k} \pmod{m_k}, \tag{4}$$

其中 $t_i = 1, 2, \cdots, T_i$; $i = 1, 2, \cdots, k$. 由(i)知(1)的解与(4)的解相同. 由孙子定理知 (4) 中每一同余式组对模 m 恰有一解，故 (2) 对模 m 有 $T_1T_2\cdots T_k$ 个解，又由上一小节定理 3 知，这 $T_1T_2\cdots T_k$ 个解对模 m 两两不同余. 故(1)对模 m 的解数是 $T = T_1T_2\cdots T_k$. 证完.

这个定理给出了，由 (2) 的解，用孙子定理即可得 (1) 的解.

例 1. 解同余式

$$f(x) = x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}. \tag{5}$$

解：由定理 1 知 (5) 与同余式组

$$f(x) \equiv 0 \pmod{5}, \qquad f(x) \equiv 0 \pmod{7}$$

等价，容易验证第一个同余式有解

$$x \equiv 1, 4 \pmod{5},$$

而第二个同余式有三个解：

$$x \equiv 3, 5, 6 \pmod{7},$$

故同余式 (5) 有 $2 \cdot 3 = 6$ 个解，即诸同余式组

$$x \equiv b_1 \pmod 5,\ x \equiv b_2 \pmod 7,\ b_1 = 1, 4,\ b_2 = 3, 5, 6$$

的解，由孙子定理得

$$x \equiv 21b_1 + 15b_2 \pmod{35}.$$

以 b_1, b_2 的值分别代入即得 (5) 的全部解：

$$x \equiv 31, 26, 6, 24, 19, 34 \pmod{35}.$$

我们已经知道任一正整数 m 可以写成标准分解式 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. 由定理 1 知，欲解同余式 $f(x) \equiv 0 \pmod m$, 只要解同余式组

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \qquad (i = 1, 2, \cdots, k).$$

因此下面就来讨论模为素数幂的同余式

$$f(x) \equiv 0 \pmod{p^\alpha}. \tag{6}$$

显然适合 (6) 的每一个整数都适合同余式

$$f(x) \equiv 0 \pmod p. \tag{7}$$

但反过来不一定成立，例如 2 是 $x^{10} - 1 \equiv 0 \pmod{11}$ 的解，但 2 不适合 $x^{10} - 1 \equiv 0 \pmod{11^2}$. 因此，(6) 的解 (如果有解) 可在 (7) 的解中找到；如果 (7) 无解，则 (6) 无解.

如何由 (7) 的解来找 (6) 的解呢？我们有

定理 2. 设 $x \equiv x_1 \pmod p$ 即

$$x = x_1 + pt_1 \qquad (t_1 = 0, \pm 1, \pm 2, \cdots) \tag{8}$$

是 (7) 的一个解，并且 $p \nmid f'(x_1)$, 这里 $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$, 则(8) 刚好给出 (6) 的一个解(对模 p^α 来说)

$$x = x_\alpha + p^\alpha t_\alpha \qquad (t_\alpha = 0, \pm 1, \pm 2, \cdots),$$

即 $x \equiv x_\alpha \pmod{p^\alpha}$, 其中 $x_\alpha \equiv x_1 \pmod p$.

证. 我们用数学归纳法来证明

(i) $\alpha = 1$, 定理显然成立.

(ii) 假定定理对 $\alpha - 1$ 的情形成立，即(8)刚好给出

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

的一个解

$$x = x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1} \qquad (t_{\alpha-1} = 0, \pm 1, \cdots),$$

$x_{\alpha-1} \equiv x_1 \pmod p$，把它代入(6)，由 $2\alpha-2 \geqslant \alpha$，可得

$$f(x_{\alpha-1}) + p^{\alpha-1}t_{\alpha-1}f'(x_{\alpha-1}) \equiv 0 \pmod{p^\alpha},$$

但 $f(x_{\alpha-1}) \equiv 0 \pmod{p^{\alpha-1}}$，因此

$$t_{\alpha-1}f'(x_{\alpha-1}) \equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}} \pmod p$$

由

$$x_{\alpha-1} \equiv x_1 \pmod p$$

即得

$$f'(x_{\alpha-1}) \equiv f'(x_1) \pmod p,$$

但

$$(f'(x_1), p) = 1,$$

于是

$$(p, f'(x_{\alpha-1})) = 1,$$

故上式恰有一解

$$t_{\alpha-1} = t'_{\alpha-1} + pt_\alpha \qquad (t_\alpha = 0, \pm 1, \cdots),$$

因此刚好给出(6)式的一解：

$$x = x_{\alpha-1} + p^{\alpha-1}(t'_{\alpha-1} + pt_\alpha) = x_\alpha + p^\alpha t_\alpha \ (t_\alpha = 0, \pm 1, \cdots),$$

其中 $x_\alpha = x_{\alpha-1} + p^{\alpha-1}t'_{\alpha-1} \equiv x_1 \pmod p$. 故定理对 α 的情形同样成立. 由归纳法，定理得证.

定理 2 的证法同时提供了一个由(7)的解求(6)的解的方法，我们举一例来说明.

例2. 解同余式

$$f(x) \equiv 0 \pmod{27}, \qquad f(x) = x^4 + 7x + 4.$$

解：$f(x) \equiv 0 \pmod 3$ 有一解 $x \equiv 1 \pmod 3$，并且 $f'(1) \not\equiv 0 \pmod 3$. 以 $x = 1 + 3t$ 代入 $f(x) \equiv 0 \pmod 9$ 得

$$f(1) + 3t_1f'(1) \equiv 0 \pmod 9.$$

但 $f(1) \equiv 3 \pmod 9$，$f'(1) \equiv 2 \pmod 9$，故

$$3 + 3t_1 \cdot 2 \equiv 0 \pmod 9), \text{ 即 } 2t_1 + 1 \equiv 0 \pmod 3,$$

因此 $t_1 = 1 + 3t_2$，而

$$x = 1 + 3(1 + 3t_2) = 4 + 9t_2$$

是 $f(x) \equiv 0 \pmod 9$ 的解，

以

$$x = 4 + 9t_2$$

代人

$$f(x) \equiv 0 \pmod{27},$$

即得

$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27},$$

即

$$18 + 9t_2 \equiv 0 \pmod{27},$$

即

$$2t_2 + 2 \equiv 0 \pmod 3,$$

则

$$t_2 = 2 + 3t_3,$$

故

$$x = 4 + 9(2 + 3t_3) = 22 + 27t_3$$

为所求的解.

2.8. 素数模的同余式 在上一节中，我们把解高次同余式的问题归结到了解素数模的高次同余式，但是我们还没有一般的方法(除了将 $0, 1, \cdots, p-1$ 逐一代入验算)去解素数模的同余式. 本节就素数模同余式的次数与解数的关系作一初步的讨论. 首先我们考虑素数模同余式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv 0 \pmod p, \qquad (1)$$

其中 p 为素数，而 $a_n \not\equiv 0 \pmod p$.

定理 1. 设 $x \equiv \alpha_i \pmod p$, $i = 1, \cdots, k$ 是(1)的 k 个 (不同的)解，则

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_k) f_k(x) \pmod p, \qquad (2)$$

其中 $f_k(x)$ 是 $n - k$ 次多项式，首项系数是 a_n.

证. 由多项式除法得

$$f(x) = (x - \alpha_1) f_1(x) + r,$$

其中 $f_1(x)$ 是首项系数为 a_n 的 $n-1$ 次多项式，r 是常数，由假设 $f(\alpha_1) \equiv 0 \pmod p$，故 $r \equiv 0 \pmod p$，因此

$$f(x) \equiv (x - \alpha_1) f_1(x) \pmod p.$$

令 $x = \alpha_i$ $(i = 2, \cdots, k)$ 得

$$0 \equiv f(\alpha_i) \equiv (\alpha_i - \alpha_1) f_1(\alpha_i) \pmod p.$$

但 $\alpha_i \not\equiv \alpha_1 \pmod p$ $(i = 2, \cdots, k)$，而 p 是素数，故

$$f_1(\alpha_i) \equiv 0 \pmod p \quad (i = 2, \cdots, k).$$

因此，显然可以用归纳法证明定理.

定理 2. 同余式 (1) 不同余的解的个数不超过它的次数.

证. 我们用反证法. 设(1)的解数超过n，则(1)至少有 $n+1$ 个解，设为

$$x \equiv \alpha_i \pmod p \quad (i = 1, \cdots, n, n+1),$$

由定理 1 得

$$f(x) \equiv a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \pmod p,$$

由于

$$0 \equiv f(\alpha_{n+1}) \equiv a_n(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n) \pmod p.$$

因为 p 为素数， $a_n \not\equiv 0 \pmod p$

故有一个 $\alpha_i (1 \leqslant i \leqslant n)$ 使 $\alpha_{n+1} - \alpha_i \equiv 0 \pmod p$，这与假设矛盾. 证完.

§3. 二 次 剩 余

解一般的二次同余式，可以归结到讨论形如

$$x^2 \equiv n \pmod m, \quad (n, m) = 1$$

的同余式. 本节的主要目的是讨论上述同余式，从而引入二次剩余和二次非剩余的概念. 此外，还将讨论同余式

$$x^k \equiv n \pmod p$$

以及引入 k 次剩余. 次数等概念.

3.1. 二次剩余和 Legendre 符号

定义. 设 m 为大于 1 的整数，假定 $(m, n) = 1$，若

$$x^2 \equiv n \pmod m$$

有解，则 n 叫做模 m 的二次剩余；若无解，则 n 叫做模 m 的二次非剩余.

这样就把和 m 互素的数分为两类，一类为二次剩余，一类为二次非剩余. 例如，1，2，4 是 7 的二次剩余，3，5，6 是 7 的二次非剩余.

下面我们首先讨论奇素数 p 的二次剩余和二次非剩余的问

题．即讨论同余式

$$x^2 \equiv n \pmod p, \quad (n,p)=1 \tag{1}$$

的解．我们有定理 1.

定理 1. 在模 p 的缩系中，有 $\frac{1}{2}(p-1)$ 个二次剩余和 $\frac{1}{2}(p-1)$ 个二次非剩余，且

$$1^2, 2^2, \cdots, \left(\frac{1}{2}(p-1)\right)^2 \tag{2}$$

就是模 p 的全部二次剩余．

证．如果 (1) 有解，则 (1) 只有两个解．这是因为 (1) 有解，设为 $x \equiv x_1 \pmod p$，则 $x \equiv -x_1 \pmod p$ 也是(1)的解，且 $x_1 \not\equiv -x_1 \pmod p$，故由 § 2.8 定理 2 知 (1) 只有两个解．显然，(1) 若有解，则必有一解 x 适合 $1 \leqslant x \leqslant \frac{1}{2}(p-1)$．所以 n 如果是模 p 的二次剩余，则 n 必和 (2) 中一个数同余，反之 (2) 中任一个数都是二次剩余，且其中任两个都不同余．故 (2) 是模 p 的全部二次剩余．同时可知模 p 的缩系中恰有 $\frac{1}{2}(p-1)$ 个二次剩余和 $\frac{1}{2}(p-1)$ 个二次非剩余．证完．

定理 2. 如果 n 是模 p 的二次剩余，则

$$n^{\frac{p-1}{2}} \equiv 1 \pmod p, \tag{3}$$

而如果 n 是模 p 的二次非剩余，则

$$n^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{4}$$

证．如果 n 是模 p 的二次剩余，则 (1) 有解 α 适合 $(\alpha, p)=1$．由 (1) 推出

$$n^{\frac{p-1}{2}} \equiv \alpha^{p-1} \equiv 1 \pmod p,$$

即 (3) 成立，再由 $n^{p-1} \equiv 1 \pmod p$ 推得

$$(n^{\frac{p-1}{2}}-1)(n^{\frac{p-1}{2}}+1) \equiv 0 \pmod p.$$

因为 p 是奇素数，所以(3)和(4)有一个而且只有一个成立．已知，

当 n 是模 p 的二次剩余时式(3)成立,由定理1和§2.8定理2知 $\frac{p-1}{2}$ 个二次剩余是同余式 $x^{\frac{p-1}{2}}\equiv 1\pmod p$ 的全部解，这样 $\frac{p-1}{2}$ 个二次非剩余是同余式 $x^{\frac{p-1}{2}}\equiv -1\pmod p$ 的全部解,故 n 是模 p 的二次剩余,则(4)成立．证完.

实际上，定理2告诉我们 n 是模 p 的二次剩余的充分必要条件是(3)成立,而 n 是模 p 的二次非剩余的充分必要条件是(4)成立.

定理2给出的判别方法在 p 比较大时,很难实际运用,现在引入 Legendre 符号,以便给出一个易于实际计算的判别方法.

定义. 设 p 为奇素数，$(p, n)=1$，令

$$\left(\frac{n}{p}\right)=\begin{cases}1, & \text{若 } n \text{ 是模 } p \text{ 的二次剩余;}\\ -1, & \text{若 } n \text{ 是模 } p \text{ 的二次非剩余.}\end{cases}$$

函数 $\left(\frac{n}{p}\right)$ 叫做 Legendre 符号.

由于 $n\equiv n'\pmod p$ 时, n 和 n' 同为二次剩余或同为二次非剩余,故有

$$\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right).$$

由定义立刻得出

$$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}\pmod p, \tag{5}$$

由(5)不难推出 Legendre 符号的下列性质:

1° $\left(\frac{1}{p}\right)=1$;

2° $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$;

3° $\left(\frac{n_1 n_2\cdots n_k}{p}\right)=\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)\cdots\left(\frac{n_k}{p}\right)$，这里 $p\nmid\prod_{i=1}^{k} n_i$,

这是因为

$$\left(\frac{n_1n_2\cdots n_k}{p}\right)\equiv(n_1n_2\cdots n_k)^{\frac{p-1}{2}}=n_1^{\frac{p-1}{2}}n_2^{\frac{p-1}{2}}\cdots n_k^{\frac{p-1}{2}}$$

$$\equiv\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)\cdots\left(\frac{n_k}{p}\right)\pmod p,$$

而左右两端上取值 ±1，故有性质 3° 成立；

4° $\left(\frac{nn_1^2}{p}\right)=\left(\frac{n}{p}\right)$.

这样，任给一个整数 n，计算$\left(\frac{n}{p}\right)$时，只需算出下面的三种值.

$$\left(\frac{-1}{p}\right),\ \left(\frac{2}{p}\right),\ \left(\frac{q}{p}\right)\quad(q\text{ 为奇素数}).$$

因为当 n 分解为 $n=\pm2^mq_1^{l_1}\cdots q_s^{l_s}$ 时，$2<q_1<\cdots<q_s$，q_i $(i=1,\cdots,s)$是素数，则

$$\left(\frac{n}{p}\right)=\left(\frac{\pm1}{p}\right)\left(\frac{2}{p}\right)^m\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s}.$$

为了计算 $\left(\frac{2}{p}\right)$，$\left(\frac{q}{p}\right)$，我们需要下述定理.

定理 3. 令 $p>2$，$(p,n)=1$，设 $\frac{1}{2}(p-1)$ 个数

$$n,\ 2n,\cdots,\ \frac{1}{2}(p-1)n\pmod p$$

的最小正余数中有 m 个大于 $\frac{1}{2}p$，则

$$\left(\frac{n}{p}\right)=(-1)^m.$$

证. 以 $a_1,\cdots,a_l$ 表示余数中小于 $\frac{1}{2}p$ 的所有数，$b_1,\cdots,b_m$，表余数中大于 $\frac{1}{2}p$ 的所有的数，显然 $l+m=\frac{1}{2}(p-1)$，且

$$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv\prod_{k=1}^{\frac{1}{2}(p-1)}kn=\left(\frac{p-1}{2}\right)!\,n^{\frac{p-1}{2}}\pmod p,\quad(6)$$

$p-b_t$ 也在 1 和 $\frac{1}{2}(p-1)$ 之间，故 a_s，$p-b_t$ $(s=1,\cdots,l,$ $t=1,\cdots,m)$ 是 1 和 $\frac{1}{2}(p-1)$ 之间的 $\frac{1}{2}(p-1)$ 个数．现证这 $\frac{1}{2}(p-1)$ 个数各不相同，只需证 $a_s \neq p-b_t$，如果 $a_s = p-b_t$，则有

$$xn + yn \equiv 0 \pmod p \quad \left(1 \leqslant x \leqslant \frac{1}{2}(p-1),\right.$$
$$\left. 1 \leqslant y \leqslant \frac{1}{2}(p-1)\right),$$

即

$$x + y \equiv 0 \pmod p,$$

此不可能，故

$$\prod_{s=1}^{l} a_s \prod_{t=1}^{m} (p-b_t) = \left(\frac{p-1}{2}\right)!.$$

由 (6) 得

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= \prod_{s=1}^{l} a_s \prod_{t=1}^{m} (p-b_t) \\ &\equiv (-1)^m \prod_{s=1}^{l} a_s \prod_{t=1}^{m} b_t \\ &\equiv (-1)^m \left(\frac{p-1}{2}\right)! \, n^{\frac{p-1}{2}} \pmod p,\end{aligned}$$

故得

$$n^{\frac{p-1}{2}} \equiv (-1)^m \pmod p.$$

由定理 2．可知

$$\left(\frac{n}{p}\right) \equiv (-1)^m \pmod p,$$

即得

$$\left(\frac{n}{p}\right) = (-1)^m. \qquad \text{证完.}$$

在定理 3 中，取 $n=2$，则

$$2,\ 2\cdot 2,\ 3\cdot 2,\ \cdots,\ \left(\frac{p-1}{2}\right)\cdot 2$$

已是模 p 的最小正余数. 现求出适合

$$\frac{p}{2}<2k<p \text{ 即 } \frac{p}{4}<k<\frac{p}{2}$$

的 k 的个数，即得 $m=\left[\frac{p}{2}\right]-\left[\frac{p}{4}\right]$.

令 $p=8a+r,\ \ r=1,3,5,7$，则得

$$m=2a+\left[\frac{r}{2}\right]-\left[\frac{r}{4}\right]\equiv 0,1,1,0 \pmod 2,$$

故得下面定理.

定理 4. 若 p 是奇素数，则

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

换句话说，若 $p\equiv\pm 1 \pmod 8$，则 2 是模 p 的二次剩余，若 $p\equiv\pm 3 \pmod 8$，则 2 是模 p 的二次非剩余.

下面给出二次互逆定理，证明略去.

定理 5. 令 $p>2,\ q>2$ 是两个素数，$p\neq q$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{4}(p-1)(q-1)},$$

或

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{1}{4}(p-1)(q-1)}.$$

3.2. Jacobi 符号 引入 Legendre 符号，运用互逆定理，可以判断二次同余式是否有解，但是要遇到把一个数 n 分解成标准分解式这个麻烦的问题，这就是运用 Legendre 符号进行计算时的缺点，去掉这一缺点的一个方法就是引进 Jacobi 符号.

定义. 设 m 是一个正奇数，$m=p_1p_2\cdots p_t$，$p_i(i=1,\cdots,t)$ 是素数 $(m,n)=1$，则

$$\left(\frac{n}{m}\right)=\prod_{i=1}^{t}\left(\frac{n}{p_i}\right)$$

叫做 Jacobi 符号.

例如，$\left(\frac{1}{m}\right)=1$，若 $(m, a)=1$，则 $\left(\frac{a^2}{m}\right)=1$.

关于它的计算法则容易得到定理 1.

定理 1. 设 m, m' 为正奇数.

1° 若 $n \equiv n' \pmod m$，和 $(n, m)=1$，则

$$\left(\frac{n}{m}\right)=\left(\frac{n'}{m}\right);$$

2° 若 $(n, m)=(n, m')=1$，则

$$\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right)=\left(\frac{n}{mm'}\right);$$

3° 若 $(n, m)=(n', m)=1$，则

$$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)=\left(\frac{nn'}{m}\right).$$

定理 2. $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

证. 因为 $\left(\frac{-1}{m}\right)=\prod_{i=1}^{t}\left(\frac{-1}{p_i}\right)=(-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}}$,

故只需证 $\sum_{i=1}^{t}\frac{p_i-1}{2}\equiv\frac{\prod_{i=1}^{t}p_i-1}{2} \pmod 2$ 就行了.

$t=1$ 显然是对的，又对任二奇数 u 和 v 有

$$\frac{u-1}{2}+\frac{v-1}{2}\equiv\frac{uv-1}{2} \pmod 2.$$

故用归纳法. 由

$$\sum_{i=1}^{t}\frac{p_i-1}{2}=\sum_{i=1}^{t-1}\frac{p_i-1}{2}+\frac{p_t-1}{2}$$

$$\equiv \frac{\prod_{i=1}^{t-1} p_i - 1}{2} + \frac{p_t - 1}{2} \equiv \frac{\prod_{i=1}^{t} p_i - 1}{2} \pmod 2$$

即得定理．证完．

定理 3. $\left(\frac{2}{m}\right) = (-1)^{\frac{1}{8}(m^2-1)}$.

证．对任二奇数 u, v 有 $(u^2-1)(v^2-1) \equiv 0 \pmod{16}$，故

$$\frac{u^2v^2-1}{8} \equiv \frac{u^2-1}{8} + \frac{v^2-1}{8} \pmod 2,$$

用定理 2 的证法可得定理．证完．

定理 4. 若 m 与 n 是二正奇数，且 $(m, n) = 1$，则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证．设 $m = \Pi p$，$n = \Pi q$，则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \left(\prod_p \prod_q \left(\frac{p}{q}\right)\right)\left(\prod_p \prod_q \left(\frac{q}{p}\right)\right)$$

$$= \prod \prod \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \prod_p \prod_q (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$= (-1)^{\sum_p \sum_q \frac{p-1}{2}\cdot\frac{q-1}{2}} =$$

$$= (-1)^{\left(\sum_p \frac{p-1}{2}\right)\left(\sum_q \frac{q-1}{2}\right)} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证完．

关于 Jacobi 符号有几点要注意：

1. 它具有 Legendre 符号一样的计算法则，没有 m 是素数的限制，n 是奇数时，也不需要把 n 分解成素因数的乘积，所以计算起来很方便．

2. 在 $t = 1$ 时，$\left(\frac{n}{m}\right)$ 的值与 Legendre 符号 $\left(\frac{n}{m}\right)$ 的值相等（这里 m 是一个奇素数）．

3. 在 $t>1$ 时，如果 $\left(\frac{n}{m}\right)=-1$，则 $x^2\equiv n\pmod m$ 无解。但当 $\left(\frac{n}{m}\right)=1$ 时，$x^2\equiv n\pmod m$ 不一定有解。

如 $\left(\frac{2}{9}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)=(-1)(-1)=1$。而同余式 $x^2\equiv 2\pmod 9$ 无解。

3.3. 二项同余式 $x^k\equiv n\pmod p$ 设 p 是素数，本节讨论二项同余式

$$x^k\equiv n\pmod p,\qquad (p,n)=1.$$

我们有定理 1.

定理 1. 同余式

$$x^k\equiv 1\pmod p \tag{1}$$

有解，且解数等于 $(k,p-1)$.

证. 设 $d=(k,p-1)$，必有二整数 s 和 t 使

$$sk+t(p-1)=d,$$

这样有 $x^d=(x^k)^s\cdot(x^{p-1})^t$. 所以 (1) 的解必为

$$x^d\equiv 1\pmod p \tag{2}$$

的解. 反过来，(2) 的解显然是 (1) 的解.

因此，我们只需证明(2)的解的个数等于 d，由 § 2.8 定理 2 知 (2) 的解数不超过 d，而

$$\frac{x^{p-1}-1}{x^d-1}=(x^d)^{\frac{p-1}{d}-1}+\cdots+x^d+1\equiv 0\pmod p$$

的解数不超过 $p-1-d$，又由 $x^{p-1}-1\equiv 0\pmod p$ 的解数是 $p-1$，所以上式的解数应是 $p-1$ 减去 (2) 的解数，故 (2) 的解数 $\geqslant d$，定理得证.

定理 2. 二项同余式

$$x^k\equiv n\pmod p \tag{3}$$

或无解，或有 $(k,p-1)$ 个解.

证. 如果(3)有一解，设为 x_0，由于$(x_0,p)=1$，所以存在 x_0'

使 $x_0x_0' \equiv 1 \pmod p$，记以 x_0^{-1} 表示这样的整数，则由(3)

$$(x_0^{-1}x)^k \equiv (x_0^{-1})^k \cdot n \equiv 1 \pmod p.$$

令 $Z = x_0^{-1}x$，这样我们就可以建立一个(3)的解集合到(1)的解集合上的映射 σ，其定义如下：

$$\sigma(x) \equiv Z, \qquad x \equiv x_0 Z \pmod p,$$

这里 x, Z 分别是(3)，(1)的解.

如果 $x_1 x_2$ 是(3)的两个解，那么 $\sigma(x_1) \equiv Z_1$, $\sigma(x_2) \equiv Z_2$，而 $x_1 \equiv x_0 Z_1$, $x_2 \equiv x_0 Z_2$，所以 $Z_1 \not\equiv Z_2 \pmod p$，即 Z_1, Z_2 是(1)的两个解. 这就证明了 σ 是一一对应的，由定理 1 知(1)的解数是 $(k, p-1)$，故(3)的解数(如有解的话)也是 $(k, p-1)$. 证完.

定理 3. 若 x 过模 p 的缩系，则 x^k 取 $\dfrac{p-1}{(k, p-1)}$ 个互不同余的值.

证. 把模 p 的缩系中 $p-1$ 个数按它们的 k 次方同余 $(\mathrm{mod}\, p)$ 的分为一类(这是一个等价关系)，这样就将 $p-1$ 个数分成了若干没有公共数同时也无遗漏的类. 由定理 2 知每一类有 $(k, p-1)$ 个模 p 不同余的数，故整个 $p-1$ 个数分成 $\dfrac{p-1}{(p-1, k)}$ 个类，每一类对应一数，模 p 互不同余. 证完.

3.4. 整数的次数 我们知道，如果 $(n, h) = 1$，则 $h^{\varphi(n)} \equiv 1 \pmod n$. 我们引进次数的概念如下.

定义. 设 h 为一整数，$(h, n) = 1$，适合

$$h^l \equiv 1 \pmod n$$

的最小正整数 l 叫做 h 对模 n 的次数，或 h 的次数，mod n.

定理 1. 设 h 的次数为 l, mod n，若 $h^m \equiv 1 \pmod n$，则 $l \mid m$.

证. 如果定理所给条件不成立，则必有两整数 q 和 r，使

$$m = ql + r \qquad (0 < r < l),$$

而

$$1 \equiv h^m = h^{ql+r} = h^{ql} \cdot h^r \equiv h^r \pmod n,$$

这就和 l 的定义相违背. 证完.

推论. 设 $(h, n)=1$，h 对模 n 的次数为 l，则 $l|\varphi(n)$.

定理 2. 如果存在一整数 a，它的次数是 l，mod p，则恰有 $\varphi(l)$ 个不同的整数，mod p，次数是 l.

证. 因为 $l|p-1$. 所以 $(l, p-1)=l$，由 § 3.3 定理 1 知，同余式

$$x^l \equiv 1 \pmod p$$

有 l 个解，它们正好是 $a, a^2, \cdots, a^l \pmod p$.

另一方面，我们来证明这 l 个解中有 $\varphi(l)$ 个次数是 l，因为当 $(r, l)=1$ 时，设 a^r 的次数是 l'，由 $a^{rl} \equiv 1 \pmod p$，故 $l'|l$；而 $a^{rl'} \equiv 1 \pmod p$，故 $l|rl'$，于是 $l|l'$. 这样便得到 $l'=l$. 反过来，若 a^r 的次数是 l，必有 $(r, l)=1$，否则，设 $(r, l)=d$，$d>1$，于是 $(a^r)^{l/d} \equiv 1 \pmod p$，$\dfrac{l}{d}<l$，和 l 的定义矛盾. 这就证明了如果存在一个整数 a，它的次数是 l，则恰有 $\varphi(l)$ 个不同的整数，mod p，次数是 l. 证完.

定理 3. 设 $l|p-1$，则次数是 l 的，模 p 互不同余的整数的个数为 $\varphi(l)$.

证. 设 $\Psi(l)$ 代表 $1, 2, \cdots, p-1$ 中次数为 $l \pmod p$ 的个数，又因为 $1, 2, \cdots, p-1$ 中任一个数的次数都等于某一个 l，$l|p-1$，故有

$$\sum_{l|p-1} \Psi(l)=p-1. \tag{1}$$

另一方面，Euler 函数有一个容易验证的性质即

$$\sum_{l|p-1} \varphi(l)=p-1. \tag{2}$$

由于定理 2 告诉我们 $\Psi(l)$ 或者等于零，或者等于 $\varphi(l)$. 从而 $\Psi(l) \leqslant \varphi(l)$，故由 (1), (2) 得到的和式

$$\sum_{l|p-1}(\varphi(l)-\Psi(l))=0$$

的每一项都是非负的，所以必须有 $\Psi(l)=\varphi(l)$. 证完.

现在给出两个便于计算次数的结果.

定理 3. 如果 $n = p_1^{l_1}\cdots p_k^{l_k}$，整数 h 模 n 的次数等于整数 h 模 $p_i^{l_i}(i = 1,\cdots,k)$ 的次数的最小公倍数.

证. 设 f_i 表示 h 模 $p_i^{l_i}$ 的次数 $(i = 1,\cdots,k)$，$d = [f_1,\cdots,f_k]$，则由

$$h^d \equiv 1 \pmod{p_i^{l_i}} \quad (i = 1,\cdots,k),$$

得

$$h^d \equiv 1 \pmod{n}.$$

如果 d 不是 h 模 n 的次数，则设 h 的次数为 d'，$d' < d$，但由

$$h^{d'} \equiv 1 \pmod{n}$$

可得

$$h^{d'} \equiv 1 \pmod{p_i^{l_i}} \qquad (i = 1,\cdots,k),$$

故 $f_i | d'(i = 1,\cdots,k)$，此与 d 是最小公倍数矛盾. 证完.

定理 4. 设 p 是一个素数，h 模 p^j 的次数是 f_j，则或者 $f_{j+1} = f_j$ 或者 $f_{j+1} = pf_j$ 且又设 $p^i \| h^{f_2} - 1$[1]，进而有

$$f_j = \begin{cases} f_2, & \text{如果 } 2 \leqslant j \leqslant i; \\ p^{j-i}f_2, & \text{如果 } j > i. \end{cases}$$

证. 因为 $h^{f_j} \equiv 1 \pmod{p^j}$，故 $(h^{f_j})^k \equiv 1 \pmod{p^j}$，且

$$\sum_{k=0}^{p-1} (h^{f_j})^k \equiv \sum_{k=0}^{p-1} 1 \equiv p \pmod{p^j} \equiv 0 \pmod{p}.$$

又有 $h^{f_j} \equiv 1 \pmod{p^j}$，故可得

$$h^{pf_j} - 1 = (h^{f_j} - 1)\left(\sum_{k=0}^{p-1} (h^{f_j})^k\right) \equiv 0 \pmod{p^{j+1}},$$

故 $f_{j+1} | pf_j$. 又因 $h^{f_{j+1}} \equiv 1 \pmod{p^j}$，故 $f_j | f_{j+1}$. 由于 p 是素数，所以或者 $f_{j+1} = f_j$，或者 $f_{j+1} = pf_j$.

由于 $p^i \| h^{f_2} - 1$，故 $f_j | f_2 (j = 2, 3,\cdots,i)$，另一方面，$f_2 | f_j$ $(j = 2, 3,\cdots,i)$，故有 $f_j = f_2$，$2 \leqslant j \leqslant i$；对于 $j > i$，则 $p^j \nmid h^{f_2} - 1$，因此 $f_{i+1} = pf_2$，$f_{i+2} = pf_{i+1} = p^2f_2$，$\cdots$，$f_j = p^{j-i}f_2$.

---

1) 符号 $a^s \| b$ 表示 $a^s | b$，$a^{s+1} \nmid b$，$s \geqslant 1$.

证完.

例. 设 $h=7$, $p=2$, 求 7 模 2^{10} 的次数 f_{10}.

由于 $f_1=1$, $f_2=2$, 且 $7^2-1=48$, $2^4\parallel 48$, 故 $f_{10}=2^{10-4}\cdot 2=128$.

3.5. 原根和指数 由 § 3.4 定理 3 知有 $\varphi(p-1)$ 个不同余的数,它们的次数是 $p-1$, mod p, 我们引进

定义. 次数是 $p-1$ 的整数叫做 p 的原根.

令 g 是 p 的一个原根,则

$$g^0, g^1, \cdots, g^{p-2} \pmod p$$

必无两个互相同余,否则设

$$g^i \equiv g^j \pmod p \qquad (0 \leqslant i < j \leqslant p-2),$$

故

$$g^i(g^{j-i}-1) \equiv 0 \pmod p,$$

于是

$$g^{j-i} \equiv 1 \pmod p.$$

故 $p-1 \mid j-i$, 这是不可能的.

由于上述原根的性质,我们有下面定义.

定义. 任一整数 n, $(n, p)=1$, 必有一数 a, 使

$$n \equiv g^a \pmod p \qquad (0 \leqslant a < p-1),$$

a 叫做 n 的指数, mod p, 以 $a=\operatorname{ind}_g n$ 表示, 在不易引起混淆的情况下,简写成 $a=\operatorname{ind} n$.

若 b 为任一整数,使

$$n \equiv g^b \pmod p,$$

显然 $b \geqslant \operatorname{ind} n$. 由

$$g^{\operatorname{ind} n}(g^{b-\operatorname{ind} n}-1) \equiv 0 \pmod p,$$

故有

$$g^{b-\operatorname{ind} n} \equiv 1 \pmod p.$$

所以

$$b \equiv \operatorname{ind} n \pmod{p-1}.$$

指数与通常的对数类似;有下面的性质:

1°. 如果 $p\nmid ab$，则

$$\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1},$$

这是因为，若设 $ab \equiv g^{\operatorname{ind} ab} \pmod p$，$a \equiv g^{\operatorname{ind} a} \pmod p$，$b \equiv g^{\operatorname{ind} b} \pmod p$，则

$$g^{\operatorname{ind} ab} \equiv ab \equiv g^{\operatorname{ind} a} \cdot g^{\operatorname{ind} b} = g^{\operatorname{ind} a+\operatorname{ind} b} \pmod p.$$

故

$$\operatorname{ind} ab \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}.$$

2°. 如 $p\nmid a$，则 $\operatorname{ind} a^l \equiv l \operatorname{ind} a \pmod{p-1}$.

这是因为，若设

$$a^l \equiv g^{\operatorname{ind} a^l}, \qquad a \equiv g^{\operatorname{ind} a} \pmod p,$$

故

$$a^l \equiv (g^{\operatorname{ind} a})^l = g^{l \operatorname{ind} a} \pmod p.$$

所以

$$\operatorname{ind} a^l \equiv l \operatorname{ind} a \pmod{p-1}.$$

对于 n 是复合数的时候，如果存在整数 g 使 g 对模 n 的次数是 $\varphi(n)$，那么这样的 g 叫做对模 n 的原根. 我们有定理 1.

定理 1. n 有原根存在的充分必要条件是 $n = 2, 4, p^l, 2p^l$. 这里 $l \geqslant 1$，p 是奇素数.

证. (i) 设 n 的标准分解式为

$$n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}, \qquad p_1 < p_2 < \cdots < p_s,$$

任一整数 a，$(a, p_i) = 1$，必适合

$$a^{\varphi(p_i^{l_i})} \equiv 1 \pmod{p_i^{l_i}},$$

令 l 是 $\varphi(p_1^{l_1}), \cdots, \varphi(p_s^{l_s})$ 的最小公倍数，则

$$a^l \equiv 1 \pmod n.$$

故如果 $l < \varphi(n)$，则 n 无原根存在. 而仅当 $\varphi(p_1^{l_1}), \cdots, \varphi(p_s^{l_s})$ 两两互素的时候 $l = \varphi(n)$. 所以，当 $p > 2$，因 $\varphi(p^l)$ 为偶数，故 n 不能有两个不同的奇素因数，即 n 有原根，n 必为 2^l，p^l，$2^c p^l$ 之一. 若 $c \geqslant 2$，$\varphi(2^c) = 2^{c-1}$，故仅有 $n = 2^l, p^l, 2p^l$ 三种可能性.

(ii) $n = 2^l$，若 $l = 1$，1 即为对模 2 的原根；若 $l = 2, 3$

即为对模 4 的原根，因为 $(a, 2) = 1$ 时，

$$a^2 \equiv 1 \pmod{2^3}，\text{若 } a^{2^{l-3}} \equiv 1 \pmod{2^{l-1}}，\text{则}$$

$$a^{2^{l-2}} = (1 + \lambda 2^{l-1})^2 = 1 + 2^l\lambda + 2^{2(l-1)}\lambda^2 \equiv 1 \pmod{2^l},$$

故由归纳法，对任一个奇数 a，当 $l \geqslant 3$ 时，

$$a^{2^{l-2}} \equiv 1 \pmod{2^l},$$

此时 $\varphi(2^l) = 2^{l-1} > 2^{l-2}$，故当 $l > 2$ 时，$n = 2^l$ 无原根.

(iii) 设 $n = p^l$，已经知道 $l = 1$ 时，p 有原根存在，设 g 为 p 的原根，如果 $g^{p-1} - 1 \not\equiv 0 \pmod{p^2}$，则取 $r = g$；若

$$g^{p-1} - 1 \equiv 0 \pmod{p^2},$$

则取 $r = g + p$，也是 p 的原根，且

$$\begin{aligned} r^{p-1} - 1 &= (g + p)^{p-1} - 1 \\ &\equiv g^{p-1} + (p-1)pg^{p-2} - 1 \\ &\equiv -pg^{p-2} \not\equiv 0 \pmod{p^2}. \end{aligned}$$

设

$$r^{p-1} - 1 = kp, \qquad p \nmid k,$$

由归纳法可证

$$(1 + kp)^{p^s} \equiv 1 + kp^{s+1} \pmod{p^{s+2}} \quad (s \geqslant 0),$$

故

$$(r^{p-1})^{p^s} = (1 + kp)^{p^s} \equiv 1 + kp^{s+1} \pmod{p^{s+2}}.$$

这里 $p \nmid k$，令 $s + 2 = l$，即得

$$r^{p^{l-2}(p-1)} \equiv 1 + kp^{l-1} \pmod{p^l} \quad (l \geqslant 2). \tag{1}$$

设 r 对模 p^l 的次数为 e，则 $e \mid \varphi(p^l) = p^{l-1}(p-1)$，又因 r 是 p 的原根，故 $p - 1 \mid e$，可设 $e = p^t(p-1)$，$0 \leqslant t \leqslant l-1$，但由 (1) 知 t 只能等于 $l - 1$，即 $e = \varphi(p^l)$，所以 r 是 p^l 的原根.

(iv) $n = 2p^l$，设 g 是 p^l 的原根. 我们来证明 g 是奇数时，也是 $2p^l$ 的原根.

因为 $(g, 2p^l) = 1$，故

$$g^{\varphi(2p^l)} \equiv 1 \pmod{2p^l}.$$

设 g 对模 $2p^l$ 的次数是 b，则

$$b \mid \varphi(2p^l) = \varphi(p^l),$$

又

$$g^{b} \equiv 1 \pmod{p^{l}},$$

则

$$\varphi(p^{l}) \mid b,$$

故

$$b = \varphi(2p^{l}).$$

如果 g 是偶数，则同理可证 $g + p^{l}$ 是模 $2p^{l}$ 的原根．证完．

判断一个整数 g 是否是 n ($n = p^{l}$ 或 $2p^{l}$) 的原根，不需要逐一计算 $g^{1}, g^{2}, \cdots, g^{\varphi(n)-1}, \pmod{n}$，而只需计算 $g^{t} \pmod{n}$，这里 $t \mid \varphi(n)$，基于这样的想法，我们有

定理 2． 设 $n > 1$，$\varphi(n)$ 的所有不同素因数是 $q_1, q_2, \cdots, q_k$，$(g, n) = 1$，则 g 是模 n 的一个原根的充分必要条件是

$$g^{\varphi(n)/q_i} \not\equiv 1 \pmod{n} \qquad (i = 1, 2, \cdots, k). \tag{1}$$

证．(i) 若 g 是模 n 的原根，则 g 对模 n 的次数是 $\varphi(n)$，但 $0 < \dfrac{\varphi(n)}{q_i} < \varphi(n)$ ($i = 1, 2, \cdots, k$)，故 (1) 成立．

(ii) 若(1)成立．设 g 对模 n 的次数是 f，假定 $f < \varphi(n)$，因 $f \mid \varphi(n)$，所以 $\dfrac{\varphi(n)}{f}$ 是大于 1 的整数，故有某个 $q_i \left| \dfrac{\varphi(n)}{f} \right.$，即 $\dfrac{\varphi(n)}{f} = q_i u$，$\dfrac{\varphi(n)}{q_i} = fu$，于是

$$g^{\varphi(n)/q_i} = g^{fu} = (g^{f})^{u} \equiv 1 \pmod{n},$$

这与(1)式矛盾，故 $f = \varphi(n)$，即 g 是模 n 的一个原根．证完．

3.6. k 次剩余　类似二次剩余的概念，一般的，我们有

定义． 设 p 是一个奇素数，$p \nmid n$，若

$$x^{k} \equiv n \pmod{p} \tag{1}$$

有解，则 n 叫做模 p 的 k 次剩余，否则叫做模 p 的 k 次非剩余．

定理 1． n 为模 p 的 k 次剩余的充分必要条件是

$$(k, p-1) \mid \operatorname{ind} n.$$

证．设 $\operatorname{ind} x = y$，$\operatorname{ind} n = a$，则由(1)的不同解一定能得到同余式

$$ky \equiv a \pmod{p-1} \tag{2}$$

的不同解;反过来,设 $x \equiv g^y \pmod{p}$, 则 x 是(1)的解,同样由(2)的不同的解一定能得到同余式(1)的不同的解. 所以同余式(1)和(2)同时有解或同时无解,并且当有解时,解的个数都是 $(k, p-1)$ 个.而(2)有解的充分必要条件是 $(k, p-1) | a$.证完.

定理 2. n 为模 p 的 k 次剩余的充分必要条件是

$$n^{p-1/(k,p-1)} \equiv 1 \pmod{p}. \tag{3}$$

证. 如果(1)有解 α, 则由(1)

$$n^{p-1/(k,p-1)} \equiv \alpha^{k \cdot \frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}.$$

反之,设(3)成立,且设

$$n \equiv g^{\operatorname{ind} n} \pmod{p},$$

g 是模 p 的一个原根,我们有

$$g^{\operatorname{ind} n \cdot \frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p},$$

故

$$p-1 \,|\, \operatorname{ind} n \cdot \frac{p-1}{(k, p-1)},$$

由此推出,

$$(k, p-1) \,|\, \operatorname{ind} n,$$

由定理 1 知 n 是模 p 的 k 次剩余. 证完.

现在我们来讨论 $k=3$ 的情形. 此时(1)为

$$x^3 \equiv n \pmod{p}, \quad (p, n) = 1, \quad p \geqslant 5. \tag{4}$$

如果 $p = 6m+5$, 则 $(3, 6m+4) = 1$, 此时(4)有解,即对任一 $p \nmid n$ 的 n 皆为模 p 的三次剩余. 如果 $p = 6m+1$, 则

$$(3, 6m) = 3,$$

此时(4)或者无解,或者有三个解.

特别地,设

$$x^3 \equiv 2 \pmod{p}, \qquad p = 6m+1, \tag{5}$$

我们有定理 3.

定理 3. (5)有解,即 2 是模 p 的三次剩余,其充分必要条件是 p 可表示为

$$p = a^2 + 27b^2, \quad a, b \text{ 是整数.}$$

以后讨论数论变换要用到这个结论．其证明，在这里就不写出了．

3.7. Fermat 数和 Mersenne 数　形如 $F_t = 2^{2^t} + 1$ 的数叫 Fermat 数．这里 $t = 0, 1, 2, \cdots$，已知前 7 个 Fermat 数是：$F_0 = 3$，$F_1 = 5$，$F_2 = 17$，$F_3 = 257$，$F_4 = 65537$，$F_5 = 641 \times 6700417$，$F_6 = 274177 \times 67280421310721$，前五个是素数．

定理 1. 任给两个 Fermat 数 F_m, F_n, $m \neq n$，则

$$(F_m, F_n) = 1.$$

证．可设 $m > n \geqslant 0$, $m = n + k$, $k > 0$，而 $l | F_n$, $l | F_{n+k}$. 如果 $x = 2^{2^n}$，我们有

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1}$$
$$= \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1,$$

故 $F_n | F_{n+k} - 2$，且 $l | F_{n+k}$, $l | F_{n+k} - 2$，推出 $l | 2$，因为 F_t 是奇数，故 $l = 1$．证完．

利用 Legendre 符号，可以证明定理 2．

定理 2. 设 $t > 1$，F_t 的每一个素因数形如

$$k 2^{t+2} + 1, \qquad k > 0.$$

证．设 $F_t = 2^{2^t} + 1$, $t > 1$, $p | F_t$, p 是素数，易知 2 对模 p 的次数是 2^{t+1}，故 $2^{t+1} / p - 1$，可设 $p = k 2^{t+1} + 1$，由 $t > 1$ 知 $p \equiv 1 \pmod 8$，于是 $\left(\frac{2}{p}\right) = 1$，而

$$1 = \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} = 2^{h 2^t} \equiv (-1)^h \pmod p,$$

故 $2 | h$．证完．

现在讨论形如 $2^n - 1$ 的数，我们有定理 3．

定理 3. 若 $2^n - 1$ 为素数．则 n 为素数．

证．当 $n = 1$ 时，$2^n - 1 = 2 - 1 = 1$，非素数．当 n 是一个复

合数时，即 $n = kl$，$1<k<n$，那么 $2^k - 1 | 2^n - 1$，而 $1 < 2^k - 1 < 2^n - 1$，故此时 $2^n - 1$ 也非素数．证完．

设 p 为素数．形如 $2^p - 1$ 的数叫 Mersenne 数，目前已知使 $M_p = 2^p - 1$ 为素数的 p 是

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937.

第二章　卷积运算和快速变换

§1. 卷积运算

在信息的数字处理中，卷积是最常见的一种运算，所谓两个复数序列 $x_n(n=0,1,\cdots,M_1-1)$，$h_n(n=0,1,\cdots,M_2-1)$ 的卷积是指：

$$y_n=\sum_{\substack{k=0\\0\leqslant n-k<M_2}}^{M_1-1}h_{n-k}x_k=\sum_{\substack{k=0\\0\leqslant n-k<M_1}}^{M_2-1}h_kx_{n-k}\qquad(1)$$

$$(n=0,1,2,\cdots,M_1+M_2-2).$$

容易看出，在 $M_1=M_2=L$ 时，算出 $y_0,y_1,\cdots,y_{2L-2}$ 共需 L^2 阶次乘法和 L^2 阶次加法，那么当 L 很大时，大量的乘、加法运算是很费时间的。于是，寻找快速计算它们的方法就是一件有意义的工作了。

通常通过循环卷积来计算(1)式．两个序列 $x_n(n=0,1,\cdots,N-1)$ 和 $h_n(n=0,1,\cdots,N-1)$ 的循环卷积定义为

$$y_n=\sum_{k=0}^{N-1}x_kh_{\langle n-k\rangle_N}=\sum_{k=0}^{N-1}x_{\langle n-k\rangle_N}h_k\qquad(2)$$

$$(n=0,1,\cdots,N-1).$$

定理．序列 $x_0,x_1,\cdots,x_{M_1-1}$ 和 $h_0,h_1,\cdots,h_{M_2-1}$ 的卷积(1)可以通过两个长为 N 的序列的循环卷积来计算，这里 $N=2^m$，且满足[1)]

$$2^{m-1}<M_1+M_2-1\leqslant 2^m.\qquad(3)$$

证．设序列

1) 因为要用快速演段，故取 $N=2^m$ 满足(3)，实际上，取 $N=M_1+M_2-1$，就可由(2)推出(1)．

$$x_i' = \begin{cases} x_i, & i = 0, 1, \cdots, M_1 - 1, \\ 0, & i = M_1, M_1 + 1, \cdots, M_1 + M_2 - 2, \cdots, N - 1. \end{cases}$$

$$h_i' = \begin{cases} h_i, & i = 0, 1, \cdots, M_2 - 1, \\ 0, & i = M_2, M_2 + 1, \cdots, M_1 + M_2 - 2, \cdots, N - 1. \end{cases}$$

由 (2)，两个序列 $x_0', x_1', \cdots, x_{N-1}'$ 和 $h_1', h_2', \cdots, h_{N-1}'$ 的循环卷积是

$$y_n' = \sum_{k=0}^{N-1} x_k' h'_{\langle n-k \rangle_N} \quad (n = 0, 1, \cdots, N-1).$$

在 $n = 0, 1, \cdots, M_1 + M_2 - 2$ 时，

$$\begin{aligned} y_n' &= \sum_{k=0}^{N-1} x_k' h'_{\langle n-k \rangle_N} = \sum_{k=0}^{M_1-1} x_k' h'_{\langle n-k \rangle_N} \\ &= \sum_{\substack{k=0 \\ 0 \leqslant n-k < M_2}}^{M_1-1} x_k' h'_{\langle n-k \rangle_N} + \sum_{\substack{k=0 \\ n-k \geqslant M_2}}^{M_1-1} x_k' h'_{\langle n-k \rangle_N} + \sum_{\substack{k=0 \\ n-k < 0}}^{M_1-1} x_k' h'_{\langle n-k \rangle_N} \\ &= \sum_{\substack{k=0 \\ 0 \leqslant n-k < M_2}}^{M_1-1} x_k' h'_{\langle n-k \rangle_N} = \sum_{\substack{k=0 \\ 0 \leqslant n-k < M_2}}^{M_1-1} x_k h_{n-k} = y_n. \end{aligned}$$

这就给出了 (1) 式.

§2. DFT

一般常用离散傅里叶变换（简称 DFT）来计算复数域上的循环卷积.

任给序列 $x_n (n = 0, 1, \cdots, N-1)$，变换

$$X_k = \sum_{n=0}^{N-1} x_n W_N^{-nk}, \ W_N = e^{2\pi i/N} \ (k = 0, 1, \cdots, N-1) \quad (1)$$

称为一个长为 N 的 DFT. 其逆离散傅里叶变换（简称 IDFT）为

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k W_N^{nk} \quad (n = 0, 1, \cdots, N-1). \quad (2)$$

(1) 和 (2) 可以写成矩阵形式

$$\begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix} = T \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix},$$

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} = U \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix},$$

这里

$$T = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N^{-1} & \cdots & W_N^{-(N-1)} \\ 1 & W_N^{-2} & \cdots & W_N^{-2(N-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & W_N^{-(N-1)} & \cdots & W_N^{-(N-1)^2} \end{pmatrix},$$

$$U = \frac{1}{N} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & W_N & \cdots & W_N^{N-1} \\ 1 & W_N^2 & \cdots & W_N^{2(N-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & W_N^{N-1} & \cdots & W_N^{(N-1)^2} \end{pmatrix}.$$

利用复数域上N次本原单位根 W_N 的下列性质:

$$\frac{1}{N}\sum_{n=0}^{N-1} W_N^{pn} = \begin{cases} 1, & \text{如果 } p \equiv 0 \pmod N, \\ 0, & \text{如果 } p \not\equiv 0 \pmod N. \end{cases}$$

不难验证 $TU = I_N$, I_N 表示N阶单位矩阵, 可见 $U = T^{-1}$. 因此(1)和(2)互为逆变换.

DFT 的重要作用在于它具有所谓的循环卷积性质.

任给两个序列 $x_0, x_1, \cdots, x_{N-1}$ 和 $h_0, h_1, \cdots, h_{N-1}$, 且设

$$X_k = \sum_{n=0}^{N-1} x_n W_N^{-nk}, \qquad H_k = \sum_{n=0}^{N-1} h_n W_N^{-nk},$$

$$Y_k = \sum_{n=0}^{N-1} y_n W_N^{-nk} \qquad (k = 0, 1, \cdots, N-1),$$

其中 y_n 由 § 1 的 (2) 式给出，则有

$$Y_k = X_k \cdot H_k \qquad (k = 0, 1, \cdots, N-1).$$

这是由于

$$\begin{aligned} X_k \cdot H_k &= \sum_{n=0}^{N-1} x_n W_N^{-nk} \cdot \sum_{l=0}^{N-1} h_l W_N^{-lk} \\ &= \sum_{n=0}^{N-1} \sum_{l=0}^{N-1} x_n h_l W_N^{-(n+l)k} \\ &= \sum_{t=0}^{N-1} \Bigg(\sum_{\substack{0 \leqslant n, l \leqslant N-1 \\ n+l \equiv t (\mathrm{mod} N)}} x_n h_l \Bigg) W_N^{-tk} \\ &= \sum_{t=0}^{N-1} \left(\sum_{n=0}^{N-1} x_n h_{\langle t-n \rangle_N} \right) W_N^{-tk} \\ &= \sum_{t=0}^{N-1} y_t W_N^{-tk} = Y_k \ (k = 0, 1, \cdots, N-1), \end{aligned}$$

由此推知循环卷积的计算可以通过两次 DFT 和一次 IDFT 来完成。

§ 3. FFT

直接按 § 2 的 (1) 式计算 DFT，求出全部 N 个 $X_k (k = 0, 1, \cdots, N-1)$ 共需 N^2 次乘法和 N^2 次加法. 当 N 很大时，运算量是相当大的. 而且由于 $x_k (k = 0, 1, \cdots, N-1)$ 一般为复数. 所以这里的乘法与加法都是指复数运算. 六十年代出现了一种计算 DFT 的新算法，它大大地减少了运算次数，这种算法通称为快速傅里叶变换，简记为 FFT. 下面介绍这一算法的基本思想. 其一般的迭代公式将在以后给出.

我们设序列的长度 $N = 2^m$. 并以 O_N 表示计算长为 N 的 DFT 所用乘加法次数，一般的，O_N 不仅与长度 N 有关，而且还与所采用的算法有关，如果直接按 § 2 的 (1) 计算，则 $O_N = N^2$. 以下我们不用这种直接算法，而将序列 $x_0, x_1, \cdots, x_{N-1}$ 依次按足标

的奇偶性分解为两个子序列：

$$\begin{cases} x_l' = x_{2l} \\ x_l'' = x_{2l+1} \end{cases} \quad \left(l = 0, 1, \cdots, \frac{N}{2} - 1\right).$$

这两个长为 $\frac{N}{2}$ 的序列 x_l' 和 x_l'' $\left(l = 0, 1, \cdots, \frac{N}{2} - 1\right)$ 的 DFT 分别为：

$$\left.\begin{aligned} X_k' &= \sum_{l=0}^{\frac{N}{2}-1} x_l' W_{\frac{N}{2}}^{-lk} \\ X_k'' &= \sum_{l=0}^{\frac{N}{2}-1} x_l'' W_{\frac{N}{2}}^{-lk} \end{aligned}\right\} \left(k = 0, 1, \cdots, \frac{N}{2} - 1\right), \tag{1}$$

因为

$$W_{\frac{N}{2}} = W_N^2, \qquad W_{\frac{N}{2}}^{-lk} = W_{\frac{N}{2}}^{-lk + \frac{lN}{2}}.$$

故

$$\begin{aligned} X_k &= \sum_{n=0}^{N-1} x_n W_N^{-nk} = \sum_{l=0}^{\frac{N}{2}-1} x_l' W_N^{-2lk} + \sum_{l=0}^{\frac{N}{2}-1} x_l'' W_N^{-(2l+1)k} \\ &= \sum_{l=0}^{\frac{N}{2}-1} x_l' W_{\frac{N}{2}}^{-lk} + W_N^k \sum_{l=0}^{\frac{N}{2}-1} x_l'' W_{\frac{N}{2}}^{-lk} \quad (k = 0, 1, \cdots, N-1), \\ &= \begin{cases} X_k' + W_N^k X_k'', & 0 \leqslant k \leqslant \frac{N}{2} - 1, \\ X_{k-\frac{N}{2}}' + W_N^k X_{k-\frac{N}{2}}'', & \frac{N}{2} \leqslant k \leqslant N - 1. \end{cases} \end{aligned} \tag{2}$$

(2) 式在计算上有重要的意义． 计算 X_k' 与 X_k'' $\left(k = 0, 1, \cdots, \frac{N}{2} - 1\right)$各需 $O_{N/2}$ 次乘加法．然后，按(2)算出 $X_k(k = 0, 1, \cdots, N - 1)$ 还需N次乘加法． 因此通过这途径求出 $X_k(k = 0, 1, \cdots, N - 1)$ 所用的乘加法次数为 $2O_{N/2} + N$. 如果直接计算(1)，则 $O_{N/2} = \left(\frac{N}{2}\right)^2$. 这时的 O_N 变为

$$O_N = 2O_{\frac{N}{2}} + N = \frac{N^2}{2} + N.$$

当N较大时，其计算量比直接计算所用的N^2次乘加法几乎减少了一半。

因为 $\frac{N}{2} = 2^{m-1}$，故又可将 x'_l 与 x''_l $\left(l = 0, 1, \cdots, \frac{N}{2} - 1\right)$ 分别分解为两个长为 $\frac{N}{4}$ 的子序列。重复上面的处理办法，可以将计算 X'_l 与 X''_l $\left(l = 0, 1, \cdots, \frac{N}{2} - 1\right)$ 所用的乘加法次数 $O_{N/2}$ 降为 $2O_{N/4} + \frac{N}{2}$。继续这一过程，直到分解出的子序列都只由两点构成。直接计算其 DFT，易知 $O_2 = 2$。于是当我们把长为N的序列分解为二元序列来计算 DFT 时，就有

$$O_N = 2O_{\frac{N}{2}} + N, \qquad O_{\frac{N}{2}} = 2O_{\frac{N}{4}} + \frac{N}{2}, \cdots,$$

$$O_4 = 2O_2 + 4, \quad O_2 = 2.$$

故得

$$O_N = 2^{m-1}O_2 + (m-1)N = mN = N\log_2 N.$$

这比直接计算所用的N^2次乘加法是大为减少了。例如 $N = 2^{10} \approx 10^3$ 时，$\frac{N\log_2 N}{N^2} = \frac{\log_2 N}{N} \approx 10^{-2}$；$N = 2^{20} \approx 10^6$ 时，$\log_2 N/N \approx 5 \times 10^{-5}$。即此时用 FFT 的计算量分别为用直接算法的计算量的百分之一和五万分之一。

§4. 素数幂变换

对于快速傅里叶变换，一般要求 DFT 的长度是 2 的方幂。但是，当 DFT 的长度是一个奇素数的方幂时，利用数论中原根的性质，可以证明，此时对 DFT 的计算可化为若干个循环卷积的计算，这通常称为素数幂变换，它提供了用循环卷积的快速算法来计算 DFT 的新途径。

设 $x_n(n=0,1,\cdots,N-1)$ 是复数域上的一个序列，熟知，一个长为N的 DFT 指

$$X_k=\sum_{n=0}^{N-1}x_nW_N^{nk}, W_N=e^{-2\pi i/N}\,(k=0,1,\cdots,N-1). \quad (1)$$

我们设 $N=p$，p 是一个奇素数，

$$\bar{X}_k=\sum_{n=1}^{p-1}x_nW_p^{nk}\quad(k=1,\cdots,p-1), \quad (2)$$

则有

$$X_0=\sum_{n=0}^{p-1}x_n,\quad X_k=x_0+\bar{X}_k\quad(k=1,\cdots,p-1). \quad (3)$$

由于 (3) 是很容易计算的简单加法，在 $N=p$ 时把 (1) 化为循环卷积的计算，通常指把 (2) 化为循环卷积的计算.

定理 1. 设 $N=p$，p 是一个奇素数，则 (2) 可用一个长为 $p-1$ 的循环卷积来计算.

证. 由于 p 是一个奇素数，其原根存在，设为 g，则 $1,2,\cdots,p-1$ 可由 $\langle g^l\rangle_p$ $(l=0,1,\cdots,p-2)$ 表示出，于是 (2) 化为

$$\bar{X}_{\langle g^l\rangle_p}=\sum_{m=0}^{p-2}x_{\langle g^m\rangle_p}W_p^{g^{l+m}}\quad(l=0,1,\cdots,p-2). \quad (4)$$

由于 $g^{p-1}\equiv 1\ (\mathrm{mod}\ p)$，所以 (4) 是两个周期为 $p-1$ 的序列 $a_u=x_{\langle g^u\rangle_p}(u=0,1,\cdots)$ 和 $b_v=W_p^{g^v}(v=0,1,\cdots)$ 的互相关函数，而此时，我们知道[1]，只需把其中一个序列重排一下，就可化为一个长为 $p-1$ 的循环卷积. 证完.

定理 2. 设 $N=p^t$，p 是一个奇素数，则 (1) 可用一个长为 $\varphi(p^t)$ 的循环卷积，二个长为 $\varphi(p^{t-1})$ 的循环卷积，$\cdots$，2^{t-1} 个长为 $\varphi(p)$ 的循环卷积来计算(除开类似(3)的简单加法). 其中 $\varphi(n)$ 为 Euler 函数.

证. 我们对素数的方幂用归纳法来证明.

设 $t=1$，即定理 1. 设 $t=h$ 时，定理成立. 我们进一步证明 $t=h+1$ 的情形. 此时 $N=p^{h+1}$，设

1) 参看本书第八章.

$$\overline{X}_k = \sum_{\substack{n=1 \\ p \nmid n}}^{p^{h+1}-1} x_n W^{kn}, \ W = W_{p^{h+1}}, \ p \nmid k(k = 1, \cdots, p^{h+1} - 1). \tag{5}$$

由于 p^{h+1} 存在原根，设为 g，则 $\varphi(p^{h+1})$ 个数 $k = 1, \cdots, p^{h+1} - 1, p \nmid k$，可由 $\langle g^u \rangle_{p^{h+1}} (u = 0, 1, \cdots, \varphi(p^{h+1}) - 1)$ 表示出，于是(5)化为

$$\overline{X}_{\langle g^l \rangle_{p^{h+1}}} = \sum_{m=0}^{\varphi(p^{h+1})-1} x_{\langle g^m \rangle_{p^{h+1}}} W^{g^{l+m}}$$
$$(l = 0, 1, \cdots, \varphi(p^{h+1}) - 1), \tag{6}$$

而(6)又可以化为一个长为 $\varphi(p^{h+1})$ 的循环卷积.

此外，尚需计算

$$X_{up} = \sum_{n=0}^{p^{h+1}-1} x_n W^{nup} (u = 0, 1, \cdots, p^h - 1) \tag{7}$$

和

$$Y_k = \sum_{\substack{n=0 \\ p \mid n}}^{p^{h+1}-1} x_n W^{kn} (p \nmid k, \ k = 1, 2, \cdots, p^{h+1} - 1), \tag{8}$$

而

$$X_k = \overline{X}_k + Y_k \ (p \nmid k, \ k = 1, 2, \cdots, p^{h+1} - 1), \tag{9}$$

显然，由(7)和(9)给出(1).

由(7)可得

$$X_{up} = \sum_{n=0}^{p^{h+1}-1} x_n W_{p^h}^{nu} = \sum_{i=0}^{p^h-1} \sum_{j=0}^{p-1} x_{jp^h+i} W_{p^h}^{iu}$$
$$(u = 0, 1, \cdots, p^h - 1), \tag{10}$$

而

$$\sum_{j=0}^{p-1} x_{jp^h+i} = u_i \qquad (i = 0, 1, \cdots, p^h - 1)$$

是简单加法运算，容易求出，这样(10)就是一个长为 p^h 的 DFT.

为了计算(8)，由于对 $S = 0, 1, \cdots, p - 1$ 均有

$$Y_{Sp^h+r} = \sum_{\substack{n=0 \\ p \mid n}}^{p^{h+1}-1} x_n W^{(Sp^h+r)n} = \sum_{n'=0}^{p^h-1} x_{n'p} W_{p^h}^{n'r}$$

$$= \overline{Y}_r (r = 0, 1, \cdots, p^h - 1), \qquad (11)$$

这样 (11) 中 $p \nmid r$ $(r = 0, 1, \cdots, p^h - 1)$, 给出了 (8) 所需要的全部值 $\overline{Y}_{Sp^h+r}$, $p \nmid r$ $(r = 0, 1, \cdots, p^h-1, S = 0, 1, \cdots, p-1)$. 显然 (11) 是一个长为 p^h 的 DFT, 故除 (6) 外, 总共还需计算两个长为 p^h 的 DFT, 由归纳假设, 知道总共还需计算 2 个长为 $\varphi(p^h)$ 的循环卷积, 2^2 个长为 $\varphi(p^{h-1})$ 的循环卷积, $\cdots$, 2^h 个长为 $\varphi(p)$ 的循环卷积(除开简单的加法不计). 证完.

以上证明也是构造性的. 下面举一个例子.

例. $N = 3^2 = 9$, 令 $W_9 = W$. (1) 可写为

$$\begin{pmatrix} X_6 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \\ X_8 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & W^1 & W^2 & W^3 & W^4 & W^5 & W^6 & W^7 & W^8 \\ 1 & W^2 & W^4 & W^6 & W^8 & W & W^3 & W^5 & W^7 \\ 1 & W^3 & W^6 & 1 & W^3 & W^6 & 1 & W^3 & W^6 \\ 1 & W^4 & W^8 & W^3 & W^7 & W^2 & W^6 & W & W^5 \\ 1 & W^5 & W & W^6 & W^2 & W^7 & W^3 & W^8 & W^4 \\ 1 & W^6 & W^3 & 1 & W^6 & W^3 & 1 & W^6 & W^3 \\ 1 & W^7 & W^5 & W^3 & W & W^8 & W^6 & W^4 & W \\ 1 & W^8 & W^7 & W^6 & W^5 & W^4 & W^3 & W^2 & W \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix},$$

(5) 式对应于

$$\begin{pmatrix} \overline{X}_1 \\ \overline{X}_2 \\ \overline{X}_4 \\ \overline{X}_5 \\ \overline{X}_7 \\ \overline{X}_8 \end{pmatrix} = \begin{pmatrix} W & W^2 & W^4 & W^5 & W^7 & W^8 \\ W^2 & W^4 & W^8 & W & W^5 & W^7 \\ W^4 & W^8 & W^7 & W^2 & W & W^5 \\ W^5 & W & W^2 & W^7 & W^8 & W^4 \\ W^7 & W^5 & W & W^8 & W^4 & W^2 \\ W^8 & W^7 & W^5 & W^4 & W^2 & W \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_4 \\ x_5 \\ x_7 \\ x_8 \end{pmatrix}. \qquad (12)$$

由于 2 是模 9 的一个原根,且当 $l = 0, 1, 2, 3, 4, 5$ 时, $\langle 2^l \rangle_9 = 1, 2, 4, 8, 7, 5$, 设 $a_m = x_{\langle 2^{6-m} \rangle_9}$, $h_n = W^{2^n}$, 则 (12) 化为长为

6 的循环卷积.

$$\bar{X}_{\langle 2^l\rangle_6}=\sum_{m=0}^{5} a_m h_{\langle l-m\rangle_6} \qquad (l=0,1,2,3,4,5),$$

即

$$\begin{pmatrix}\bar{X}_1\\ \bar{X}_2\\ \bar{X}_4\\ \bar{X}_8\\ \bar{X}_7\\ \bar{X}_5\end{pmatrix}=\begin{pmatrix}W & W^5 & W^7 & W^8 & W^4 & W^2\\ W^2 & W & W^5 & W^7 & W^8 & W^4\\ W^4 & W^2 & W & W^5 & W^7 & W^8\\ W^8 & W^4 & W^2 & W & W^5 & W^7\\ W^7 & W^8 & W^4 & W^2 & W & W^5\\ W^5 & W^7 & W^8 & W^4 & W^2 & W\end{pmatrix}\begin{pmatrix}x_1\\ x_5\\ x_7\\ x_8\\ x_4\\ x_2\end{pmatrix}.$$

(7) 对应于

$$\begin{pmatrix}X_0\\ X_3\\ X_6\end{pmatrix}=\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & W^3 & W^6 & 1 & W^3 & W^6 & 1 & W^3 & W^6\\ 1 & W^6 & W^3 & 1 & W^6 & W^3 & 1 & W^6 & W^3\end{pmatrix}\begin{pmatrix}x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ x_6\\ x_7\\ x_8\end{pmatrix},$$

因为 $W^3=W_3$, (10) 对应为

$$\begin{pmatrix}X_0\\ X_3\\ X_6\end{pmatrix}=\begin{pmatrix}1 & 1 & 1\\ 1 & W_3 & W_3^2\\ 1 & W_3^2 & W_3\end{pmatrix}\begin{pmatrix}x_0+x_3+x_6\\ x_1+x_4+x_7\\ x_2+x_5+x_8\end{pmatrix},$$

而 (11) 对应为

$$\begin{pmatrix}Y_0\\ Y_1\\ Y_2\end{pmatrix}=\begin{pmatrix}Y_3\\ Y_4\\ Y_5\end{pmatrix}=\begin{pmatrix}Y_6\\ Y_7\\ Y_8\end{pmatrix}=\begin{pmatrix}1 & 1 & 1\\ 1 & W_3 & W_3^2\\ 1 & W_3^2 & W_3\end{pmatrix}\begin{pmatrix}x_0\\ x_3\\ x_6\end{pmatrix},$$

于是

$$\begin{pmatrix} X_1 \\ X_2 \\ X_4 \\ X_5 \\ X_7 \\ X_8 \end{pmatrix} = \begin{pmatrix} \overline{X}_1 \\ \overline{X}_2 \\ \overline{X}_4 \\ \overline{X}_5 \\ \overline{X}_7 \\ \overline{X}_8 \end{pmatrix} + \begin{pmatrix} Y_1 \\ Y_2 \\ Y_1 \\ Y_2 \\ Y_1 \\ Y_2 \end{pmatrix}.$$

对于 $N = 2p^l$, p 是一个奇素数. 可以证明, 此时不计简单的加法, (1) 仍可化为循环卷积运算.

§5. WFTA

在七十年代中期, Winograd 等对某些序列的 DFT 又提出了一种新的算法,它进一步把所用乘法的次数降为 $O(N)$ 阶,而加法次数大体保持在与 FFT 相当的水平. 这种算法通常称为 WFTA. 下面只对 WFTA 作一简要介绍,而不列出结果的证明.

我们知道长为N的 DFT 的矩阵表示式为

$$\mathbf{X} = T_N \mathbf{x}. \tag{1}$$

这里

$$\mathbf{X} = \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}, T_N = (W_N^{ir}) \ (i, r = 0, \cdots, N-1).$$

所谓变换矩阵 T_N 的一个标准分解式是指有

$$S_N C_N R_N = T_N, \tag{2}$$

其中 R_N 是一个 $J \times N$ 阶的关联矩阵(即它的元素仅取值 0, ± 1), C_N 是一个 $J \times J$ 阶的对角矩阵, S_N 是一个 $N \times J$ 阶的关联矩阵.

将 T_N 的标准分解式 (2) 代入 (1) 即得

$$\mathbf{X} = S_N C_N R_N \mathbf{x}, \tag{3}$$

利用关联矩阵的特性,从(3)容易推出计算(1)的乘法次数就等于对角矩阵 C_N 的阶数 J.

如果允许 J 取较大的数，那么标准分解式 (2) 是不难得到的．不失一般性，下面以 $N=3$ 的情形为例，说明 $J=N^2$ 时，分解式 (2) 一定存在．

当 $N=3$ 时，这时取

$$S_3=\begin{pmatrix}1&1&1&0&0&0&0&0&0\\0&0&0&1&1&1&0&0&0\\0&0&0&0&0&0&1&1&1\end{pmatrix},\qquad R_3=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&0\\0&1&0\\0&0&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix},$$

$$C_3=\begin{pmatrix}W_3^0&&&&&&&&\\&W_3^0&&&&&&\mathbf{0}&\\&&W_3^0&&&&&&\\&&&W_3^0&&&&&\\&&&&W_3^1&&&&\\&&&&&W_3^2&&&\\&&&&&&W_3^0&&\\&\mathbf{0}&&&&&&W_3^2&\\&&&&&&&&W_3^1\end{pmatrix},$$

就有

$$S_3C_3R_3=T_3.$$

当 J 很大时，分解式(2)对节省计算量没有多大意义，WFTA 的思想就是寻求分解式 (2) 中的可能存在的最小的 J．对于小的 $N=2,3,4,5,7,8,16$，Winograd 应用域论的方法证明了此时有 $J\sim N$．这表明对这些小 N 计算 DFT 只需 $O(N)$ 阶乘法．而且其加法个数也与 FFT 大体相当，

例．当 $N\approx 3$ 时，不难验算有

$$T_3=\begin{pmatrix}1&1&0\\1&1&1\\1&1&-1\end{pmatrix}\begin{pmatrix}1&0&0\\1&-\frac{3}{2}&0\\0&0&-\frac{i\sqrt{3}}{2}\end{pmatrix}\begin{pmatrix}1&1&1\\0&1&1\\0&1&-1\end{pmatrix}.$$

对于一些较大的 N，可以通过小 N 算法来计算 DFT. Winograd 证明了下面的结果

定理. 如果 $N=N_L N_{L-1}\cdots N_1$，$(N_i, N_j)=1$ $(i\neq j)$ 那么有

$$\mathbf{X}'=(T_{N_L}*T_{N_{L-1}}*\cdots*T_{N_1})\mathbf{x}', \tag{4}$$

这里 $\mathbf{X}'$, $\mathbf{x}'$ 是适当调整 $\mathbf{X}$ 与 $\mathbf{x}$ 的分量的次序得到的. $*$ 表示矩阵的 Kroneckes 乘积.

矩阵的 Kroneckes 乘积的运算规则为

$$A=(a_{ij})_{m\times n}, \qquad B=(b_{ij})_{s\times t},$$

则

$$A*B=\begin{pmatrix} a_{11}B\cdots a_{1n}B \\ \cdots\cdots\cdots\cdots \\ a_{m1}B\cdots a_{mn}B \end{pmatrix}$$

是一个 $ms\times nt$ 阶的矩阵.

它的一个有用的性质是

$$AB*CD=(A*C)(B*D). \tag{5}$$

如果 (4) 中的每一个因子 N_i 恰是前面所列出的小 N 中的一个，那么 T_{N_i} 就有一个低阶的标准分解式

$$T_{N_i}=S_{N_i}C_{N_i}R_{N_i} \qquad (i=1,\cdots,L).$$

将上式代入 (4) 并应用 (5) 得

$$\begin{aligned}\mathbf{X}'&=(S_{N_L}C_{N_L}R_{N_L}*S_{N_{L-1}}C_{N_{L-1}}R_{N_{L-1}}*\cdots*S_{N_1}C_{N_1}R_{N_1})\mathbf{x}'\\&=(S_{N_L}*S_{N_{L-1}}*\cdots*S_{N_1})(C_{N_L}*C_{N_{L-1}}*\cdots*C_{N_1})\\&\quad\times(R_{N_L}*R_{N_{L-1}}*\cdots*R_{N_1})\mathbf{x}',\end{aligned}$$

或简写为

$$\mathbf{X}'=S_N C_N R_N \mathbf{x}'. \tag{6}$$

不难看出 (6) 中的 S_N, R_N 是关联矩阵，C_N 是一个对角矩阵.

所以如果计算一个小 N_i 的 DFT 需用 M_i 个乘法，那么计算 (6) 所需乘法总数为

$$M=M_L M_{L-1}\cdots M_1.$$

最后，举一个例子说明这种组合过程.

$$N=12=3\times 4,\qquad W=W_{12}=e^{-\pi i/6}.$$

这时 (1) 式表示为

$$\begin{bmatrix} X_0\\ X_1\\ X_2\\ X_3\\ X_4\\ X_5\\ X_6\\ X_7\\ X_8\\ X_9\\ X_{10}\\ X_{11} \end{bmatrix} = \begin{bmatrix}
W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0\\
W^0 & W^1 & W^2 & W^3 & W^4 & W^5 & W^6 & W^7 & W^8 & W^9 & W^{10} & W^{11}\\
W^0 & W^2 & W^4 & W^6 & W^8 & W^{10} & W^0 & W^2 & W^4 & W^6 & W^8 & W^{10}\\
W^0 & W^3 & W^6 & W^9 & W^0 & W^3 & W^6 & W^9 & W^0 & W^3 & W^6 & W^9\\
W^0 & W^4 & W^8 & W^0 & W^4 & W^8 & W^0 & W^4 & W^8 & W^0 & W^4 & W^8\\
W^0 & W^5 & W^{10} & W^3 & W^8 & W^1 & W^6 & W^{11} & W^4 & W^9 & W^2 & W^7\\
W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6\\
W^0 & W^7 & W^2 & W^9 & W^4 & W^{11} & W^6 & W^1 & W^8 & W^3 & W^{10} & W^5\\
W^0 & W^8 & W^4 & W^0 & W^8 & W^4 & W^0 & W^8 & W^4 & W^0 & W^8 & W^4\\
W^0 & W^9 & W^6 & W^3 & W^0 & W^9 & W^6 & W^3 & W^0 & W^9 & W^6 & W^3\\
W^0 & W^{10} & W^8 & W^6 & W^4 & W^2 & W^0 & W^{10} & W^8 & W^6 & W^4 & W^2\\
W^0 & W^{11} & W^{10} & W^9 & W^8 & W^7 & W^6 & W^5 & W^4 & W^3 & W^2 & W^1
\end{bmatrix} \begin{bmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ x_6\\ x_7\\ x_8\\ x_9\\ x_{10}\\ x_{11} \end{bmatrix}$$

适当调整 $\mathbf{X}$ 与 $\mathbf{x}$ 分量之顺序可得

$$\left[\begin{array}{c} X_0\\ X_3\\ X_6\\ X_9\\ \hline X_4\\ X_7\\ X_{10}\\ X_1\\ \hline X_8\\ X_{11}\\ X_2\\ X_5 \end{array}\right] = \left[\begin{array}{cccc|cccc|cccc}
W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0 & W^0\\
W^0 & W^3 & W^6 & W^9 & W^0 & W^3 & W^6 & W^9 & W^0 & W^3 & W^6 & W^9\\
W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6 & W^0 & W^6\\
W^0 & W^9 & W^6 & W^3 & W^0 & W^9 & W^6 & W^3 & W^0 & W^9 & W^6 & W^3\\
\hline
W^0 & W^0 & W^0 & W^0 & W^4 & W^4 & W^4 & W^4 & W^8 & W^8 & W^8 & W^8\\
W^0 & W^3 & W^6 & W^9 & W^4 & W^7 & W^{10} & W^1 & W^8 & W^{11} & W^2 & W^5\\
W^0 & W^6 & W^0 & W^6 & W^4 & W^{10} & W^4 & W^{10} & W^8 & W^2 & W^8 & W^2\\
W^0 & W^9 & W^6 & W^3 & W^4 & W^1 & W^{10} & W^7 & W^8 & W^5 & W^2 & W^{11}\\
\hline
W^0 & W^0 & W^0 & W^0 & W^8 & W^8 & W^8 & W^8 & W^4 & W^4 & W^4 & W^4\\
W^0 & W^3 & W^6 & W^9 & W^8 & W^{11} & W^2 & W^5 & W^4 & W^7 & W^{10} & W^1\\
W^0 & W^6 & W^0 & W^6 & W^8 & W^2 & W^8 & W^2 & W^4 & W^{10} & W^4 & W^{10}\\
W^0 & W^9 & W^6 & W^3 & W^8 & W^5 & W^2 & W^{11} & W^4 & W^1 & W^{10} & W^7
\end{array}\right] \left[\begin{array}{c} x_0\\ x_9\\ x_6\\ x_3\\ \hline x_4\\ x_1\\ x_{10}\\ x_7\\ \hline x_8\\ x_5\\ x_2\\ x_{11} \end{array}\right],$$

或简记上式为

$$\mathbf{X}'=T'_{12}\mathbf{x}'. \tag{7}$$

如我们再令

$$\mathbf{y}_0=\begin{pmatrix}x_0\\x_9\\x_6\\x_3\end{pmatrix},\quad \mathbf{y}_1=\begin{pmatrix}x_4\\x_1\\x_{10}\\x_7\end{pmatrix},\quad \mathbf{y}_2=\begin{pmatrix}x_8\\x_5\\x_2\\x_{11}\end{pmatrix},$$

$$\mathbf{Y}_0=\begin{pmatrix}X_0\\X_3\\X_6\\X_9\end{pmatrix},\quad \mathbf{Y}_1=\begin{pmatrix}X_4\\X_7\\X_{10}\\X_1\end{pmatrix},\quad \mathbf{Y}_2=\begin{pmatrix}X_8\\X_{11}\\X_2\\X_5\end{pmatrix},$$

则 (7) 式变为

$$\begin{pmatrix}Y_0\\Y_1\\Y_2\end{pmatrix}=\begin{pmatrix}W^0T_4 & W^0T_4 & W^0T_4\\W^0T_4 & W^4T_4 & W^8T_4\\W^0T_4 & W^8T_4 & W^4T_4\end{pmatrix}\begin{pmatrix}y_0\\y_1\\y_2\end{pmatrix}.$$

利用 $W^4=W_{12}^4=W_3^1$，即得

$$\mathbf{X}'=(T_3*T_4)\mathbf{x}'.$$

这时再代入 T_3 与 T_4 的标准分解式就得到最后的分解式 (6) 了。

第三章　数论变换的理论基础

前一章,已经介绍了复数域上的卷积运算和 DFT, FFT 等概念.本章主要介绍数论变换的基本理论.其中心思想就是把复数域上的上述概念一一推广到模 M 的整数剩余类环 Z_M 上去讨论.

§1. 数论变换和快速数论变换

类似复数域上的情形

定义. 两个 Z_M 上的序列 $x_n(n=0,1,\cdots,N-1)$ 和 h_n $(n=0,1,\cdots,N-1)$ 的循环卷积是指

$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\quad(n=0,1,\cdots,N-1),\qquad(1)$$

这里的运算都是在环 Z_M 中进行.

定义. 设 $x_i\in Z_M(i=0,1,\cdots,N-1)$, 如果作用在序列 $x_0,x_1,\cdots,x_{N-1}$ 上的一个变换

$$X_k=\sum_{n=0}^{N-1}x_n\alpha^{nk}\quad(k=0,1,\cdots,N-1),\ \alpha\in Z_M,\qquad(2)$$

不但具有如下形状之逆变换

$$x_n=N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{-nk}\quad(n=0,1,\cdots,N-1),\qquad(3)$$

而且具有循环卷积性质. 则称(2)给出的变换为 Z_M 上一个长为 N 的数论变换或一个 Z_M 上的 DFT, 或简记为 NTT[1].

所谓变换(2)有循环卷积性质仍然指:

任给 Z_M 上的两个序列 $x_0,x_1,\cdots,x_{N-1}$ 和 $h_0,h_1,\cdots,h_{N-1}$,

---

1) 以后将证明逆变换的形状(3)可由定义中其余条件推出.

且设

$$X_k = \sum_{n=0}^{N-1} x_n \alpha^{nk}, \qquad H_k = \sum_{n=0}^{N-1} h_n \alpha^{nk},$$

$$Y_k = \sum_{n=0}^{N-1} y_n \alpha^{nk} \qquad (k = 0, 1, \cdots, N-1),$$

其中 y_n 由(1)给出，则有

$$Y_k = X_k \cdot H_k \qquad (k = 0, 1, \cdots, N-1).$$

$N = 1$ 的序列的讨论是没有意思的，故以后假定 $N \geqslant 2$.

定理 1. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$, Z_M 上长为 N 的数论变换存在的充分必要条件是 Z_M 中有元素 α 满足:

1. α 是 Z_M 中的一个 N 次单位根.
2. α 模 p_i 的次数是 $N (i = 1, \cdots, s)$.

证. 首先证明必要性. 设变换(2)之逆变换为(3), 故 N^{-1} 存在. 由循环卷积性质知

$$Y_k = X_k \cdot H_k \qquad (k = 0, 1, \cdots, N-1).$$

而

$$X_k \cdot H_k = \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} x_l h_m \alpha^{(m+l)k},$$

$$Y_k = \sum_{t=0}^{N-1} x_t h_{\langle -t \rangle_N} + \sum_{n=1}^{N-1} y_n \alpha^{nk}$$

$$= x_0 h_0 + \sum_{t=1}^{N-1} x_t h_{N-t} + \sum_{n=1}^{N-1} y_n \alpha^{nk}.$$

故由 $Y_1 = X_1 \cdot H_1$ 和序列的任意性可得 $\alpha^N = 1$, 即 α 是 N 次单位根.

因为变换(3)的系数矩阵必为(2)的系数矩阵的逆阵. 从而可推出

$$\sum_{j=0}^{N-1} (\alpha^r)^j = 0 \qquad (r = 1, 2, \cdots, N-1).$$

由此进而必须有

$$p_i \nmid \alpha^r - 1 \qquad (r = 1, 2, \cdots, r-1;\ i = 1, 2, \cdots, s),$$

否则，将有某一对 p_i 和 r，使 $p_i|\alpha^r-1$ 成立，而由 $p_i\left|\sum_{j=0}^{N-1}(\alpha^r)^j\right.$ 推出 $p_i|N$，这与 N^{-1} 存在矛盾. 这就证明了 α 模 p_i 的次数为 N.

其次证明充分性. 设 α 是 Z_M 上的 N 次单位根，则

$$
\begin{aligned}
X_k\cdot H_k &= \sum_{l=0}^{N-1}\sum_{m=0}^{N-1} x_l h_m \alpha^{(l+m)k} \\
&= \sum_{\substack{0\leq l,m\leq N-1\\ l+m=0}} x_l h_m + \sum_{\substack{0\leq l,m\leq N-1\\ l+m=N}} x_l h_m \\
&\quad + \left[\sum_{\substack{0\leq l,m\leq N-1\\ l+m=1}} x_l h_m + \sum_{\substack{0\leq l,m\leq N-1\\ l+m=N+1}} x_l h_m\right]\alpha^k + \cdots \\
&\quad + \left[\sum_{\substack{0\leq l,m\leq N-1\\ l+m=N-2}} x_l h_m + \sum_{\substack{0\leq l,m\leq N-1\\ i+m=2N-2}} x_l h_m\right]\alpha^{(N-2)k} \\
&\quad + \sum_{\substack{0\leq l,m\leq N-1\\ l+m=N-1}} x_l h_m \alpha^{(N-1)k} \\
&= y_0 + y_1\alpha^k + \cdots + y_{N-2}\alpha^{(N-2)k} + y_{N-1}\alpha^{(N-1)k} = Y_k.
\end{aligned}
$$

又由

$$(\alpha^r-1)\sum_{j=0}^{N-1}(\alpha^r)^j = \alpha^{rN}-1=0$$

和

$$p_i\nmid\alpha^r-1 \quad (r=1,\cdots,N-1;i=1,\cdots,s),$$

可推出

$$\sum_{j=0}^{N-1}(\alpha^r)^j=0 \qquad (r=1,2,\cdots,N-1).$$

再由 $N|p_i-1$ $(i=1,2,\cdots,s)$ 知 N^{-1} 存在，故(2)有形状如(3)之逆变换. 证完.

定理 2. 设 $M=p_1^{l_1}\cdots p_s^{l_s}$，$Z_M$ 上长为 N 的数论变换存在的充分必要条件是 $N|O(M)$，这里 $O(M)=(p_1-1,\cdots,p_s-1)$.

证. 如果 Z_M 上长为 N 的数论变换存在，则由定理 1 知 $N|p_i-1(i=1,\cdots,s)$，即得 $N|O(M)$.

反之，如果 $N|O(M)$，则 $N|p_i-1$ $(i=1,\cdots,s)$，故 Z_M

中 N^{-1} 存在，且存在 α_i 模 $p_i^{l_i}$ 的次数是 $N(i=1,\cdots,s)$，由孙子定理知，存在 α 是 Z_M 的 N 次单位根，且

$$\alpha \equiv \alpha_i (\bmod\ p_i^{l_i}) \qquad (i=1,\cdots,s).$$

此 α 模 p_i 的次数必须是 $N(i=1,\cdots,s)$，否则，存在某一对 p_i 和 r $(1 \leqslant r \leqslant N-1)$，使 $p_i | \alpha^r - 1$，但是由

$$(\alpha^r - 1)\sum_{j=0}^{N-1}(\alpha^r)^j \equiv 0 (\bmod p_i^{l_i}), \qquad p_i^{l_i} \nmid \alpha^r - 1,$$

故

$$p_i \Big| \sum_{j=0}^{N-1}(\alpha^r)^j,$$

于是推出 $p_i | N$，与 $N | p_i - 1$ 矛盾。证完。

推论. Z_M 上的数论变换的最大长度为 $N = O(M)$.

要使数论变换具有快速计算的效果，通常需要满足三个条件：

1. 长度 N 适合具有 FFT 类型的快速计算，对二进制的计算机来说，N 最好是 2 的方幂.

2. 由于需要进行大量的乘 α 的运算，所以，选择数论变换中的 α 之二进制表示的位数越少越好. 当然以 α 是 2 的方幂最理想.

3. 为了便于在机器上进行模 M 的运算，选取 M 之二进制表示的位数愈少愈好.

我们把和 FFT 一样的快速演段用来计算满足以上条件的数论变换的整个过程叫做快速数论变换.

§2. 数论变换的具体构造

上节给出了 Z_M 上数论变换存在性的两个判别法则. 当 $M = p_1^{l_1}\cdots p_s^{l_s}$ 和 $N(N|O(M))$ 给定后. 我们提供下面两种求 α 的具体算法，而且所有满足定理条件的 α 都可由此得到.

算法一

首先求出 β_i，使 β_i 模 p_i 的次数是 $N(i=1,\cdots,s)$，然后求

d_i 使

$$\alpha_i^N = (\beta_i + d_i p_i)^N \equiv 1 \pmod{p_i^{l_i}} \qquad (i = 1, \cdots, s).$$

这里 d_i 可按照下面的方法逐步求出. 可设 $l_i > 1$, $p_i^{t_i} \| \beta_i^N - 1$, 如果 $t_i \geqslant l_i$, 则 $d_i = 0$, 如果 $t_i \leqslant l_i - 1$, 则令 $\beta_i^N - 1 = e_i p_i^{t_i}$, $p_i \nmid e_i$, 求出 v_i 使

$$(\beta_i + v_i p_i^{t_i})^N = \beta_i^N + N\beta_i^{N-1} v_i p_i^{t_i} + \binom{N}{2} \beta_i^{N-2} v_i^2 p_i^{2t_i} + \cdots$$
$$\equiv 1 \pmod{p_i^{t_i+1}}$$

成立. 上式推出 v_i 必须且只需满足下式

$$e_i + N\beta_i^{N-1} v_i \equiv 0 \pmod{p_i},$$

而 $p_i \nmid N\beta_i^{N-1}$, 故 v_i 存在. 如果 $t_{i+1} = l_i$, 则 d_i 已经求出; 如果 $t_i + 1 < l_i$, 则重复上面的步骤,通过有限步计算后可求出 d_i.

最后由孙子定理,求出适合

$$\alpha \equiv \alpha_i \pmod{p_i^{l_i}} \qquad (i = 1, \cdots, s)$$

的 α, 此 α 即为所求.

算法二

设 β_i 模 p_i 的次数是 N, 令 $\alpha_i = \beta_i^{p_i^{l_i-1}}$, 可以证明 α_i 模 $p_i^{l_i}$ 的次数也是 N. 为此,设 $\beta_i^N = 1 + q_i p_i$, 则

$$\alpha_i^N = (\beta_i^{p_i^{l_i-1}})^N = (1 + q_i p_i)^{p_i^{l_i-1}}$$
$$= 1 + \sum_{k=1}^{p_i^{l_i-1}} \binom{p_i^{l_i-1}}{k} (q_i p_i)^k.$$

又设

$$p_i^{b_k} \| \binom{p_i^{l_i-1}}{k} (q_i p_i)^k \quad (k = 1, \cdots, p_i^{l_i-1}),$$

则

$$b_k \geqslant l_i - 1 + k - \sum_{\lambda=1}^{\infty} \left[\frac{k}{p_i^\lambda}\right] \geqslant l_i - 1 + k - \sum_{\lambda=1}^{\infty} \frac{k}{p_i^\lambda}$$
$$= l_i - 1 + k - \frac{k}{p_i - 1} > l_i - 1.$$

故 $\alpha_i^N \equiv 1 \pmod{p_i^{l_i}}$, 又 $\beta_i^{p_i^{l_i-1}} \equiv \beta_i \pmod{p_i}$, 即知 α_i 模 $p_i^{l_i}$ 的次数是 N. 然后再由孙子定理从

$$\alpha \equiv \alpha_i \pmod{p_i^{l_i}} \qquad (i = 1, 2, \cdots, s)$$

求出 α，此 α 即为所求.

由算法二和前节定理可得下面的定理.

定理. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$，$N | O(M)$，则共有 $\varphi(N)^s$ 个模 M 互不同余的 α 可构成 Z_M 上长为 N 的数论变换.

证. 由 $N | p_i - 1$ $(i = 1, \cdots, s)$ 知恰有 $\varphi(N)$ 个模 p_i 互不同余的数 $\beta_{i,1}, \cdots, \beta_{i,\varphi(N)}$，它们模 p_i 的次数都是 N $(i = 1, \cdots, s)$. 由算法二可知对任一组数

$$\beta_{1,j_1}, \cdots, \beta_{s,j_s}, \quad 1 \leqslant j_u \leqslant \varphi(N) \quad (u = 1, \cdots, s)$$

均可得到一个 α. 且易知由不同的两组数所得到的 α 模 M 必不同余. 这就证明了至少有 $\varphi(N)^s$ 个模 M 互不同余的 α 可构成 Z_M 上长为 N 的数论变换.

反之，由 § 1 定理 1，知道数论变换

$$X_k = \sum_{n=0}^{N-1} x_n \alpha^{nk} \qquad (k = 0, 1, \cdots, N-1)$$

中的 α 必定适合下面 $\varphi(N)^s$ 个同余式组之一：

$$\alpha \equiv \beta_{1,j_1} \pmod{p_1}, \ \alpha \equiv \beta_{2,j_2} \pmod{p_2}, \cdots, \ \alpha \equiv \beta_{s,j_s} \pmod{p_s},$$

$$1 \leqslant j_u \leqslant \varphi(N) \qquad (u = 1, 2, \cdots, s).$$

现在，来证明凡是适合同一个同余式组的满足 § 1 定理 1 条件的所有 α 均与模 M 同余.

设 α_1，α_2 适合定理条件，且适合同一个同余式组

$$\alpha \equiv \beta_{1,j_1^0} \pmod{p_1}, \cdots, \qquad \alpha \equiv \beta_{s,j_s^0} \pmod{p_s}.$$

由于有

$$\alpha_1^N \equiv 1 \pmod{M}, \qquad \alpha_2^N \equiv 1 \pmod{M}.$$

故 α_1，α_2 均适合

$$x^N \equiv 1 \pmod{p_i^{l_i}} \qquad (i = 1, \cdots, s). \tag{1}$$

且易知 α_1，α_2 模 $p_i^{l_i}$ $(i = 1, \cdots, s)$ 的次数均为 N，故

$$\alpha_1, \alpha_1^2, \cdots, \alpha_1^N$$

模 $p_i^{l_i}$ 互不同余，且都是(1)的解. 而对每个 i $(1 \leqslant i \leqslant s)$，$x^N \equiv$

$1 \pmod{p_i^{l_i}}$ 恰有 $(N, \varphi(p_i^{l_i})) = N$ 个解.从而 $\alpha_1, \alpha_1^2, \cdots, \alpha_1^N$ 即是 $x^N \equiv 1 \pmod{p_i^{l_i}}$ 的全部解. 故应有

$$\alpha_2 \equiv \alpha_1^{f_i} \pmod{p_i^{l_i}}, \quad 1 \leqslant f_i \leqslant N \quad (i = 1, \cdots, s),$$

故得

$$\alpha_2 \equiv \alpha_1^{f_i} \pmod{p_i} \qquad (i = 1, \cdots, s).$$

但是

$$\alpha_2 \equiv \alpha_1 \equiv \beta_{i, j_i^0} \pmod{p_i} \qquad (i = 1, \cdots, s).$$

故 $\beta_{i,j_i^0} \equiv \beta_{i,j_i^0}^{f_i} \pmod{p_i}$, 即 $\beta_{i,j_i^0}^{f_i - 1} \equiv 1 \pmod{p_i}$, 所以 $N | f_i - 1$, 于是 $f_i = 1$ $(i = 1, \cdots, s)$. 从而 $\alpha_2 \equiv \alpha_1 \pmod{M}$, 这就证明了最多有 $\varphi(N)^s$ 个模M互不同余的α可构成 Z_M 上长为N的数论变换. 证完.

例. 设 $M = 5^2 \cdot 13^2$, $N = 4$, 求其全部数论变换. 由前面的定理,知 Z_M 上共有 $\varphi(4)^2 = 4$ 个长为 4 的数论变换. 现用上面的两个算法求出其相应的四个 α.

算法一

易知 2, 3 模 5 的次数为 4; 5, 8 模 13 的次数为 4.

$$\frac{2^4 - 1}{5} = 3, \quad 3 + d_1 \cdot 8 \cdot 4 \equiv 0 \pmod 5, \quad d_1 = 1,$$

得 $5 + 2 = 7$;

$$\frac{3^4 - 1}{5} = 16, \quad 16 + d_2 \cdot 27 \cdot 4 \equiv 0 \pmod 5, \quad d_2 = 3,$$

得 $5 \cdot 3 + 3 = 18$.

7 和 18 模 5^2 的次数是 4.

$$\frac{5^4 - 1}{13} = 48, \quad 48 + d_1 \cdot 125 \cdot 4 \equiv 0 \pmod{13}, \quad d_1 = 5,$$

得 $13 \cdot 5 + 5 = 70$;

$$\frac{8^4 - 1}{13} = 315, \quad 315 + d_2 \cdot 512 \cdot 4 \equiv 0 \pmod{13}, \quad d_2 = 7,$$

得 $13 \cdot 7 + 8 = 99$.

70 和 99 模 13^2 的次数是 4.

再用孙子定理求出 4 个 α 是 268，1282，2943，和 3957.

算法二

由

$$2^5 \equiv 7 \pmod{5^2}, \qquad 3^5 \equiv 18 \pmod{5^2};$$
$$5^{13} \equiv 70 \pmod{13^2}, \quad 8^{13} \equiv 99 \pmod{13^2}.$$

再应用孙子定理也得出上述四个 α.

§3. Fermat 数变换

形如 $M = 2^b + 1$ 的数有可能满足快速数论变换所要求的条件，特别是当 $b = 2^t$，即 $M = 2^{2^t} + 1$ 为 Fermat 数. 本节我们来讨论这样的变换.

以 $M = 2^b + 1$，$b = 2^t$ 为模的数论变换叫做 Fermat 数变换，简记为 FNT. 下面来构造几个具体的 FNT.

1）当 $0 \leqslant t \leqslant 4$ 时，F_t 全是素数，这样

$$O(F_t) = F_t - 1 = 2^{2^t} \qquad (0 \leqslant t \leqslant 4).$$

故对于任意的 $N = 2^m$，$m \leqslant 2^t$ 都存在一个 FNT.

因为 3 是形如 $2^{2^t} + 1$ 的素数的一个原根，故在 $0 \leqslant t \leqslant 4$，$N = 2^{2^t}$，$\alpha = 3$ 时，可构成快速 FNT.

2）特别是由于 $2^{2^{t+1}} \equiv 1 \pmod{F_t}$，且 2 对素数 p 的次数是 2^{t+1}，这里 $p | 2^{2^t} + 1$. 又 $(2^{t+1}, 2^{2^t} + 1) = 1$，故 $M = F_t$，$N = 2^{t+1}$，$\alpha = 2$ 时，可构成快速 FNT.

3）$t \geqslant 2$ 时，对任意的 F_t，都有 $2^{t+2} | O(F_t)$，又 $(2^{t+2}, F_t) = 1$，故有 $M = F_t$，$N = 2^{t+2}$ 的 FNT 存在. 现在给出它所对应的 α，将它记为 $\alpha_{2^{t+2}}$，来证明

$$\alpha_{2^{t+2}} = 2^{2^{t-2}}(2^{2^{t-1}} - 1).$$

因为 $\alpha_{2^{t+2}}^2 \equiv 2 \pmod{F_t}$，故常记 $\alpha_{2^{t+2}} = \sqrt{2}$. 由于 $(\sqrt{2})^{2^{t+2}} \equiv 2^{2^{t+1}} \equiv 1 \pmod{F_t}$. 容易证明对 F_t 的每一个素因子 p，$\sqrt{2}$ 对 p 的次数也是 2^{t+2}.

对于计算 $M = F_t$，$N = 2^{t+2}$，$\alpha = \sqrt{2}$ 这一类快速 FNT，

乘 α 的偶数次方幂的计算较简单；乘 α 的奇数次方幂时需要乘一次 $\sqrt{2}$，而 $\sqrt{2}$ 的二进制表示是一个二位数，故比计算 $\alpha = 2$ 时的快速 FNT 之计算量要略大一些.

列出几个具体构成快速 FNT 的参数如下：

$$
\begin{array}{lll}
M = 2^4 + 1, & N = 8, & \alpha = 2; \\
M = 2^4 + 1, & N = 16, & \alpha = \sqrt{2}; \\
M = 2^8 + 1, & N = 16, & \alpha = 2; \\
M = 2^8 + 1, & N = 32, & \alpha = \sqrt{2}; \\
M = 2^8 + 1, & N = 256, & \alpha = 3; \\
M = 2^{16} + 1, & N = 32, & \alpha = 2; \\
M = 2^{16} + 1, & N = 64, & \alpha = \sqrt{2}; \\
M = 2^{16} + 1, & N = 65536, & \alpha = 3; \\
M = 2^{32} + 1, & N = 64, & \alpha = 2; \\
M = 2^{32} + 1, & N = 128, & \alpha = \sqrt{2}; \\
M = 2^{64} + 1, & N = 128, & \alpha = 2; \\
M = 2^{64} + 1, & N = 256, & \alpha = \sqrt{2}.
\end{array}
$$

§4. 用快速数论变换计算循环卷积

当我们用快速数论变换计算整数序列 x_n 和 h_n($n = 0, 1, \cdots, N-1$) 的循环卷积时，最后得到的是

$$y_n \equiv \sum_{k=0}^{N-1} x_k h_{\langle n-k \rangle_N} (\bmod M) \quad (n = 0, 1, \cdots, N-1). \qquad (1)$$

因此，用数论变换计算出的结果在普通的整数范围内是不唯一的. 那么，正确的答案是什么呢？只有解决了这个问题，NTT 才能实际运用. 现在我们就来解决这个问题. 在数字滤波的多数情况下，h_n 表示脉冲响应，其值和输入信号 x_n 的最大值通常是已知的. 因此，我们能够适当选取 M 使得下式成立，

$$|y_n| \leqslant \min\left\{ |x_n|_{\max} \sum_{k=0}^{N-1} |h_k|, \; |h_n|_{\max} \sum_{k=0}^{N-1} |x_k| \right\} < \frac{M}{2} \qquad (2)$$

$$(n=0,1,\cdots,N-1).$$

由于任一整数 a 可以唯一地表示成 $a\equiv r_a \pmod M$，$|r_a|<\frac{M}{2}$，r_a叫做 a 模M的绝对最小剩余．因此，利用快速数论变换计算出（1）式后，只要取计算结果的绝对最小剩余，即取

$$\left|\sum_{k=0}^{N-1} x_k h_{\langle n-k\rangle_N}\right|<\frac{M}{2},$$

则由（2）可知

$$y_n=\sum_{k=0}^{N-1} x_k h_{\langle n-k\rangle_N} \quad (n=0,1,\cdots,N-1).$$

这样就可得出整数序列 x_n，$h_n(n=0,1,\cdots,N-1)$ 的循环卷积的正确值来．

由此可见，在计算卷积的过程中，参加运算的所有整数均可以模M且用它及与 a 同余的任何数代替它，只要在最后得出的关于y_n的结果中，取它的绝对最小剩余就行了．为便于上机，我们对计算过程中参与运算的数都取它们模 M 的非负最小剩余，即取 Z_M 中的元素$0,1,\cdots,M-1$．

下面举一个 $N=4$ 的例子，它能帮助我们更清楚地掌握数论变换的概念，由于未用快速计算，故并不说明计算的快速效果．

求序列 $x_0=1$，$x_1=0$，$x_2=2$，$x_3=-2$ 和 $h_0=1$，$h_1=-1$，$h_2=0$，$h_3=-2$ 的循环卷积．易知$|y_n|\leqslant 8$ $(n=0,1,2,3)$，故可取$M=F_2=17$．已知 4 是Z_{17}中的 4 次本原单位根，故变换矩阵

$$T=\begin{pmatrix}1&1&1&1\\1&4&4^2&4^3\\1&4^2&4^4&4^6\\1&4^3&4^6&4^9\end{pmatrix}\equiv\begin{pmatrix}1&1&1&1\\1&4&16&13\\1&16&1&16\\1&13&16&4\end{pmatrix}\pmod{17},$$

因 $4^{-1}=13$，故

$$T^{-1} = 4^{-1}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 4^{-1} & 4^{-2} & 4^{-3} \\ 1 & 4^{-2} & 4^{-4} & 4^{-6} \\ 1 & 4^{-3} & 4^{-6} & 4^{-9} \end{pmatrix} \equiv 13\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 13 & 16 & 4 \\ 1 & 16 & 1 & 16 \\ 1 & 4 & 16 & 13 \end{pmatrix} \pmod{17},$$

$$\mathbf{X} \equiv T\begin{pmatrix} 1 \\ 0 \\ 2 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 7 \\ 5 \\ 8 \end{pmatrix} \pmod{17},$$

$$\mathbf{H} \equiv T\begin{pmatrix} 1 \\ 16 \\ 0 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 5 \\ 4 \\ 14 \end{pmatrix} \pmod{17}.$$

对应元素相乘得

$$\mathbf{Y} \equiv \begin{pmatrix} 15 \\ 1 \\ 3 \\ 10 \end{pmatrix} \pmod{17},$$

于是

$$T^{-1}\mathbf{Y} \equiv \begin{pmatrix} 3 \\ 12 \\ 6 \\ 11 \end{pmatrix} \pmod{17}.$$

取绝对最小剩余即得两个序列的循环卷积是

$$y_0 = 3, \quad y_1 = -5, \quad y_2 = 6, \quad y_3 = -6.$$

§5. 三项式变换

我们知道，有两类数论变换构成快速 FNT，一类是 $M = 2^{2^t} + 1$，$N = 2^{t+1}$，$\alpha = 2$，一类是 $M = 2^{2^t} + 1$，$N = 2^{t+2}$，$\alpha = \sqrt{2}$，它们均可快速地进行计算．但缺点是随着序列长度N

的增加，计算机的字长也增加很快（这里，序列长度N与字长$b=2^t$的关系是$N=2b$或$N=4b$）．为了克服这一缺点，方法之一是寻找数论变换，使其进行快速演段时，与快速FNT比较，使字长减少，而计算量增加不多．

所谓三项式变换，是指$M=2^{n_1}+2^{n_2}+1$是素数的数论变换．我们将从下面一些简单的定理给出某些三项式变换．

定理 1．设奇素数p的原根是g，$2^m|p-1$，则

$$M=p,\quad N=2^m,\quad \alpha=g^{\frac{p-1}{N}},$$

给出一个数论变换．

证．由于α模p的次数是N，再用§2定理1便可得证．

定理 2．有2^{m-1}个参数为$M=p$，$N=2^m$的数论变换，其对应的α可设为$\alpha_t=\langle(g^{\frac{p-1}{2^m}})^t\rangle_p$　$(t=1,3,\cdots,2^m-1)$则有

$$\alpha_{2^{m-1}+j}=p-\alpha_j\qquad(j=1,3,\cdots,2^{m-1}-1).\tag{1}$$

证．因为g是原根，故$g^{\frac{p-1}{2}}\equiv-1\pmod p$，于是有

$$\begin{aligned}\alpha_{2^{m-1}+j}&\equiv(g^{\frac{p-1}{2^m}})^{2^{m-1}+j}\equiv g^{\frac{p-1}{2}}\cdot(g^{\frac{p-1}{2^m}})^j\equiv-\langle(g^{\frac{p-1}{2^m}})^j\rangle_p\\&\equiv p-\alpha_j\pmod p\qquad(j=1,3,\cdots,2^{m-1}-1),\end{aligned}$$

故(1)式成立．证完．

由定理2知，在求全部变换时，只需求出$\alpha_1,\alpha_3,\cdots,\alpha_{2^{m-1}-1}$，剩下一半由(1)便可得出．

定理 3．设p是奇素数，g是p的原根，$2^m|p-1$，$\alpha_t=\langle(g^{\frac{p-1}{2^m}})^t\rangle_p$，则

$$\langle\alpha_1^2\rangle_p,\ \langle\alpha_3^2\rangle_p,\cdots,\ \langle\alpha_{2^{m-1}-1}^2\rangle_p,\tag{2}$$

给出了参数为$M=p$，$N=2^{m-1}$的全部数论变换的α．

证．α模p的次数是2^m，显然，α^2模p的次数是2^{m-1}，(2)有2^{m-2}个数．剩下只需证明(2)中没有两个模p同余．否则有

$$\alpha_i^2\equiv\alpha_j^2\pmod p,\tag{3}$$

$i<j$是$1,3,\cdots,2^{m-1}-1$中的某两个数．由(3)将推出$\alpha_i\equiv$

$-\alpha_j \pmod p$，故有 $(g^{\frac{p-1}{2^m}})^{j-i}+1\equiv 0 \pmod p$，从而推出

$$2^{m-1} \mid j-i,$$

这是矛盾的，故(3)式不能成立．证完．

设 $M=2^{n_1}+2^{n_2}+1=p(0<n_2<n_1)$，应用以上三个定理算出 $p<5\cdot 10^3$，$N=2^m$，$m\geqslant 5$，α 是 2 的方幂或 $\sqrt{2}$ 的全部三项式变换是：

$$M=2^7+2^6+1=193,\quad N=2^5,\quad \alpha=8;$$
$$M=2^9+2^7+1=641,\quad N=2^7,\quad \alpha=\sqrt{2};$$
$$N=2^6,\quad \alpha=2;\quad N=2^6,\quad \alpha=32;$$
$$N=2^6,\quad \alpha=128;\quad N=2^6,\quad \alpha=512;$$
$$N=2^5,\quad \alpha=4;\quad N=2^5,\quad \alpha=64;$$
$$M=2^9+2^8+1=769,\quad N=2^7,\quad \alpha=8;$$
$$N=2^7,\quad \alpha=512;\quad N=2^6,\quad \alpha=64;$$
$$M=2^{10}+2^7+1=1153,\quad N=2^5,\quad \alpha=512.$$

利用第一章 § 3.6 定理 3 给出的 2 是模 $p(p=6m+1)$ 的三次剩余的充分必要条件，可以证明

定理 4． 设素数 $p=2^{m+1}+2^m+1$，2 对模 p 的次数为 $e_2(p)$，则 $3\mid e_2(p)$．

证．设 $3\nmid e_2(p)$，便有 $e_2(p)\left|\frac{p-1}{3}\right.$，于是 $2^{\frac{p-1}{3}}\equiv 1 \pmod p$，但由第二章 § 3.6 定理 2 知 2 是模 p 的三次剩余，但 $2^{m+1}+2^m+1$ 不能表示成[1] a^2+27b^2，故应有 $3\mid e_2(p)$．证完．

以下列出 10 个 2 对模 $2^{n+1}+2^n+1$（是素数时）的次数：

---

1) 用第五章中有关二次域的结果，可证如

$$2^{m+1}+2^m+1=a^2+27b^2,$$

则在 $R(\sqrt{-3})$ 中可分解为共轭的素因子的乘积

$$(1-2^m+2^{m+1}\omega)(1-2^m+2^{m+1}\omega')=(a-3b+6b\omega)(a-3b+6b\omega'),$$

这里

$$\omega=\frac{1+\sqrt{-3}}{2},\qquad \omega'=\frac{1-\sqrt{-3}}{2},$$

而 $R(\sqrt{-3})$ 中的单位数是 ± 1，$\pm\omega$，$\pm\omega'$，易知上式不能成立．

n	$2^{n+1}+2^n+1=p$(素数)	$e_2(p)$
1	7	3
2	13	$12=3\cdot 2^2$
5	97	$48=3\cdot 2^4$
6	193	$96=3\cdot 2^5$
8	769	$384=3\cdot 2^7$
12	12289	$6144=3\cdot 2^{11}$
18	786433	$393216=3\cdot 2^{17}$
30	3221225473	$805306368=3\cdot 2^{28}$
36	206158430209	$103079215104=3\cdot 2^{35}$
41	6597069766657	$1649267441664=3\cdot 2^{39}$.

这也构成 10 个特殊的三项式变换，利用它们显然还可得到另外 8 个三项式变换:

$M=97,\quad N=2^4,\quad \alpha=8;$

$M=193,\quad N=2^5,\quad \alpha=8;$

$M=769,\quad N=2^7,\quad \alpha=8;$

$M=12289,\quad N=2^{11},\quad \alpha=8;$

$M=786433,\quad N=2^{17},\quad \alpha=8;$

$M=3221225473,\quad N=2^{28},\quad \alpha=8;$

$M=206158430209,\quad N=2^{35},\quad \alpha=8;$

$M=6597069766657,\quad N=2^{39},\quad \alpha=8;$

其中第二个和第三个已在前面给出.

§6. 二维数论变换

在运用数字电子计算机进行信息处理中，当信号与噪声是二元函数时，就需要用二维的卷积运算. 因此有必要将一维数论变换推广到二维的情形. 另外，用二维 Fermat 数变换来计算长序列的一维卷积，还可以减少所需计算机的字长.

两个二维序列 x_{n_1,n_2}, h_{n_1,n_2} ($n_1=0,1,\cdots,N_1-1$, $n_2=0$,

$1, \cdots, N_2-1$）的循环卷积是指

$$y_{n_1, n_2} = \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} x_{k_1, k_2} h_{\langle n_1-k_1 \rangle_{N_1}, \langle n_2-k_2 \rangle_{N_2}}$$

$$= \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} x_{\langle n_1-k_1 \rangle_{N_1}, \langle n_2-k_2 \rangle_{N_2}} h_{k_1, k_2} \tag{1}$$

$$(n_i = 0, 1, \cdots, N_i - 1, i = 1, 2).$$

现在引入二维数论变换的定义。

设 x_{i_1, i_2} 和 $h_{i_1, i_2} \in Z_M$（$i_1 = 0, 1, \cdots, N_1 - 1$，$i_2 = 0, 1, \cdots, N_2 - 1$），$\alpha \in Z_M$，$\beta \in Z_M$。记

$$X_{k_1, k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1, n_2} \alpha^{n_1 k_1} \beta^{n_2 k_2}, \tag{2}$$

$$H_{k_1, k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} h_{n_1, n_2} \alpha^{n_1 k_1} \beta^{n_2 k_2}, \tag{3}$$

$$Y_{k_1, k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} y_{n_1, n_2} \alpha^{n_1 k_1} \beta^{n_2 k_2}, \tag{4}$$

以上 $k_1 = 0, 1, \cdots, N_1 - 1$；$k_2 = 0, 1, \cdots, N_2 - 1$，而（4）中的 y_{n_1, n_2} 由（1）式定义。

如果对任意二维序列 x_{i_1, i_2}，（2）均有逆变换[1)]

$$x_{n_1, n_2} = N_1^{-1} N_2^{-1} \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} X_{k_1, k_2} \alpha^{-n_1 k_1} \beta^{-n_2 k_2} \tag{5}$$

（$n_1 = 0, 1, \cdots, N_1 - 1$；$n_2 = 0, 1, \cdots, N_2 - 1$），且对任意 x_{i_1, i_2} 和 h_{i_1, i_2} 均满足

$$Y_{k_1, k_2} = X_{k_1, k_2} \cdot H_{k_1, k_2} (k_i = 0, 1, \cdots, N_i - 1, i = 1, 2), \tag{6}$$

则称（2）给出的变换是 Z_M 上的一个二维数论变换。

如果 N_1，N_2 中有一个为 1，则变为一维的情形。故以下讨论均设 $N_1 > 1$，$N_2 > 1$。

定理 1. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$，（2）是 Z_M 上一个二维数论变换

1) 能够证明逆变换的形状（5）可由定义的其余条件推出。

的充分必要条件是(2)中的α和β分别是Z_M中的N_1次和N_2次单位根,且α和β模p_i的次数分别为N_1和N_2 ($i = 1, \cdots, s$)。

证. 由(2)和(3)

$$X_{k_1, k_2} \cdot H_{k_1, k_2} = \sum_{l_1=0}^{N_1-1} \sum_{l_2=0}^{N_2-1} \sum_{m_1=0}^{N_1-1} \sum_{m_2=0}^{N_2-1} x_{l_1, l_2} h_{m_1, m_2} \alpha^{(l_1+m_1)k_1} \beta^{(l_2+m_2)k_2}, \quad (7)$$

由(4)和(1)

$$\begin{aligned} Y_{k_1, k_2} &= \sum_{t_1=0}^{N_1-1} \sum_{t_2=0}^{N_2-1} x_{t_1, t_2} h_{\langle -t_1 \rangle_{N_1}, \langle -t_2 \rangle_{N_2}} + \cdots \\ &= x_{0,0} h_{0,0} + x_{0,1} h_{0, N_2-1} + x_{1,0} h_{N_1-1, 0} + \cdots. \end{aligned}$$

如果(2)满足(6),则有$Y_{0,1} = X_{0,1} \cdot H_{0,1}$和$Y_{1,0} = X_{1,0} \cdot H_{1,0}$,再由序列的任意性就可分别推得$\beta^{N_2} = 1$和$\alpha^{N_1} = 1$. 因此,$\alpha, \beta$分别是$N_1$次和$N_2$次单位根。

又若(2)的逆变换具有(5)的形状,则N_1^{-1}, N_2^{-1}必须存在,且代(2)入(5)后应有

$$\begin{aligned} x_{n_1, n_2} &= N_1^{-1} N_2^{-1} \sum_{k_1=0}^{N_1-1} \sum_{k_2=0}^{N_2-1} \sum_{l_1=0}^{N_1-1} \sum_{l_2=0}^{N_1-1} x_{l_1, l_2} \alpha^{(l_1-n_1)k_1} \beta^{(l_2-n_2)k_2} \\ &= N_1^{-1} N_2^{-1} \sum_{l_1=0}^{N_1-1} \sum_{l_2=0}^{N_2-1} x_{l_1, l_2} \left(\sum_{k_1=0}^{N_1-1} \alpha^{(l_1-n_1)k_1} \sum_{k_2=0}^{N_2-1} \beta^{(l_2-n_2)k_2} \right), \end{aligned}$$

故必须有

$$\sum_{j=0}^{N_1-1} (\alpha^r)^j = 0 \qquad (r = 1, \cdots, N_1 - 1),$$

$$\sum_{j=0}^{N_2-1} (\beta^u)^j = 0 \qquad (u = 1, \cdots, N_2 - 1).$$

再由N_1^{-1}, N_2^{-1}存在,可推出 $p_i \nmid \alpha^r - 1$ ($r = 1, \cdots, N_1 - 1$, $i = 1, \cdots, s$), $p_k \nmid \beta^u - 1$ ($u = 1, \cdots, N_2 - 1$, $u = 1, \cdots, s$). 否则,有某对p_i, r或某对p_k, u存在使 $p_i | \alpha^r - 1$ 或 $p_k | \beta^u - 1$,从而由$p_i \Big| \sum_{j=0}^{N_1-1} (\alpha^r)^j$, $p_k \Big| \sum_{j=0}^{N_2-1} (\beta^u)^j$将推出矛盾结果$p_i | N_1$或$p_k | N_2$. 必要性已证明。

现在证明充分性．由于 α 和 β 分别是 N_1 次和 N_2 次单位根，由(7)有

$$X_{k_1,k_2}\cdot H_{k_1,k_2}=\sum_{t_1=0}^{N_1-1}\sum_{t_2=0}^{N_2-1}\sum_{\substack{0\leqslant l_1,m_1\leqslant N_1-1\\ l_1+m_1\equiv t_1(\operatorname{mod}N_1)}}\times\sum_{\substack{0\leqslant l_2,m_2\leqslant N_2-1\\ l_2+m_2\equiv t_2(\operatorname{mod}N_2)}}x_{l_1,l_2}h_{m_1,m_2}\alpha^{t_1k_1}\beta^{t_2k_2}$$

$$=\sum_{t_1=0}^{N_1-1}\sum_{t_2=0}^{N_2-1}y_{t_1,t_2}\alpha^{t_1k_1}\beta^{t_2k_2}=Y_{k_1,k_2}.$$

故(6)式满足．

由 α, β 模 p_i 的次数分别为 N_1, $N_2(i=1,\cdots,s)$, 知 $(N_1N_2, M)=1$, 故 N_1^{-1}, N_2^{-1} 存在，从而可作出(5)，再由

$$(\alpha^r-1)\sum_{j=0}^{N_1-1}(\alpha^r)^j=\alpha^{rN_1}-1=0,$$

$$p_i\nmid\alpha^r-1\qquad(r=1,\cdots,N_1-1;\ i=1,\cdots,s)$$

和

$$(\beta^u-1)\sum_{j=0}^{N_2-1}(\beta^u)^j=\beta^{uN_2}-1=0,$$

$$p_k\nmid\beta^u-1\qquad(u=1,\cdots,N_2-1;\ k=1,\cdots,s)$$

可分别推出

$$\sum_{j=0}^{N_1-1}(\alpha^r)^j=0\qquad(r=1,\cdots,N_1-1),$$

$$\sum_{j=0}^{N_2-1}(\beta^u)^j=0\qquad(u=1,\cdots,N_2-1).$$

故知(5)为(2)的逆变换．证完．

类似一维的情况，我们有

定理 2. 设 $M=p_1^{l_1}\cdots p_s^{l_s}$, 变换(2)是 Z_M 上一个二维数论变换的充分必要条件是 $[N_1,N_2]\,|\,O(M)$, 这里 $O(M)=(p_1-1,\cdots,p_s-1)$.

在具体构造二维数论变换时，α 和 β 可按照§3给出的两种方

法进行计算．并且有下述定理．

定理 3. 设 $M=p_1^{l_1}\cdots p_s^{l_s}$，当 N_1 与 N_2 给定，且 $[N_1, N_2]|O(M)$，那么由(2)给出的 Z_M 上的全部二维数论变换的个数为 $\varphi(N_1)^s\varphi(N_2)^s$.

由于这两个定理的证明与一维情况类似，所以其证明过程就从略了．

§7. 用二维快速数论变换计算一维卷积

在§6的二维数论变换(2)中，设 $N_1=2^{m_1}$, $N_2=2^{m_2}$, $m_1\geqslant 1$, $m_2\geqslant 1$，再设 $N_1\times N_2$ 个和式为

$$U_{0,k_2}=\sum_{n_2=0}^{N_2-1}x_{0,n_2}\beta^{n_2k_2},\cdots,\quad U_{N_1-1,k_2}=\sum_{n_2=0}^{N_2-1}x_{N_1-1,k_2}\beta^{n_2k_2}\tag{1}$$

$$(k_2=0,1,\cdots,N_2-1),$$

则用类似 FFT 的快速演段求出(1)的全部值共需 $N_1N_2\log_2 N_2$ 次乘,加法运算．由§6的(2)知

$$X_{k_1,0}=\sum_{n_1=0}^{N_1-1}U_{n_1,0}\alpha^{n_1k_1},\cdots,\quad X_{k_1,N_2-1}=\sum_{n_1=0}^{N_1-1}U_{n_1,N_2-1}\alpha^{n_1k_1}\tag{2}$$

$$(k_1=0,1,\cdots,N_1-1).$$

应用类似 FFT 的快速演段求出(2)的全部值又需 $N_2N_1\log_2 N_1$ 次乘,加法运算．故求出全部 $N_2\times N_1$ 个值 X_{k_1,k_2} ($k_1=0,1,\cdots,N_1-1$; $k_2=0,1,\cdots,N_2-1$) 总共需要

$$N_1N_2\log_2 N_2+N_2N_1\log_2 N_1=N_1N_2\log_2 N_1N_2\tag{3}$$

次乘、加法运算．

§6的(2)还可表示成矩阵的形式

$$\begin{pmatrix} X_{0,0}\cdots X_{0,N_2-1}\\ X_{1,0}\ \cdots X_{1,N_2-1}\\ \cdots\cdots\cdots\cdots\cdots\\ X_{N_1-1,0}\cdots X_{N_1-1,N_2-1}\end{pmatrix}=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha & \cdots & \alpha^{N_1-1}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{N_1-1} & \cdots & \alpha^{(N_1-1)^2}\end{pmatrix}$$

$$\cdot\begin{pmatrix} x_{0,0} & \cdots & x_{0,N_2-1} \\ x_{1,0} & \cdots & x_{1,N_2-1} \\ \cdots & \cdots & \cdots \\ x_{N_1-1,0} & \cdots & x_{N_1-1,N_2-1} \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta & \cdots & \beta^{N_2-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{N_2-1} & \cdots & \beta^{(N_2-1)^2} \end{pmatrix}, \tag{4}$$

由(4)也可以直接得出(3). 从上面的分析可知,可用一维的快速迭代法来计算二维数论变换,这就叫二维快速数论变换.

今设 $x_0, x_1, \cdots, x_{N-1}$; $h_0, h_1, \cdots, h_{N-1}$ 是 Z_M 上的两个一维序列,其循环卷积为

$$y_n = \sum_{k=0}^{N-1} x_k h_{\langle n-k\rangle_N} \quad (n = 0, 1, \cdots, N-1). \tag{5}$$

当

$$N = 2^m,\ m \geqslant 3,\ N = N_1N_2,\ N_1 \leqslant N_2,\ N_i = 2^{s_i},\ s_i \geqslant 1, \tag{6}$$

$i = 1, 2$ 时,作二维序列

$$x_{n_1,n_2} = \begin{cases} x_{n_1+n_2N_1} & (n_1=0, 1, \cdots, N_1-1;\ n_2=0, 1, \cdots, N_2-1), \\ 0 & (n_1=N_1, \cdots, 2N_1-1;\ n_2=0, 1, \cdots, N_2-1), \end{cases} \tag{7}$$

$$h_{n_1,n_2} = h_{\langle n_1+(n_2-1)N_1\rangle_N}$$
$$(n_1=0, 1, \cdots, 2N_1-1;\ n_2=0, 1, \cdots, N_2-1) \tag{8}$$

求其二维循环卷积

$$y_{n_1,n_2} = \sum_{k_1=0}^{2N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1,k_2} h_{\langle n_1-k_1\rangle_{2N_1},\langle n_2-k_2\rangle_{N_2}}$$
$$(n_1 = 0, 1, \cdots, 2N_1-1;\ n_2 = 0, 1, \cdots, N_2-1).$$

注意,当 $n_1 = 0, 1, \cdots, N_1-1$; $n_2 = 0, 1, \cdots, N_2-1$ 时,

$$\begin{aligned} y_{N_1+n_1,n_2} &= \sum_{k_1=0}^{2N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1,k_2} h_{\langle N_1+n_1-k_1\rangle_{2N_1},\langle n_2-k_2\rangle_{N_2}} \\ &= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1,k_2} h_{\langle N_1+n_1-k_1\rangle_{2N_1},\langle n_2-k_2\rangle_{N_2}} \\ &= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1+k_2N_1} h_{N_1+n_1-k_1,\langle n_2-k_2\rangle_{N_2}} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1+k_2N_1} h_{\langle N_1+n_1-k_1+\langle n_2-k_2\rangle_{N_2}N_1-N_1\rangle_N} \\
&= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1} x_{k_1+k_2N_1} h_{\langle n_1+n_2N_1-(k_1+k_2N_1)\rangle_N} \\
&= \sum_{l=0}^{N-1} x_l h_{\langle n_1+n_2N_1-l\rangle_N} \\
&= y_{n_1+n_2N_1},
\end{aligned}
$$

故(5)的全部值可由此给出. 如果采用二维快速数论变换，易知算出(5)的全部值需要 $2N_1N_2 + 3\cdot 2N_1N_2\log_2 N_1N_2 = O(N\log_2 N)$ 阶次乘、加法运算.

对 $M = 2^b + 1$, $b = 2^t$, 则用一维快速数论变换可卷积的序列的最大长度是 $N = 4b$, 即 $M = 2^b + 1$, $N = 4b$, $\alpha = \sqrt{2}$; 而若对同一 $M = 2^b+1$, 当 $2N_1 = N_2 = 4b$, $\alpha = \beta = \sqrt{2}$ 且 $N = N_1N_2$ 满足(6)时，用二维快速 Fermat 数变换计算一维卷积，可卷积的序列长度就是 $N = 8b^2$, 若取 $2N_1 = N_2 = 2b$, $\alpha = \beta = 2$, 则可卷积的序列长度是 $N = 2b^2$.

反之，对给定之一维序列的长度 $N = 2^{m_0}$, 以 t_0 表示适合

$$
2^{2^t-1} \geqslant \min\left\{\max_{0\leqslant i\leqslant N-1}|x_i|\cdot\sum_{n=0}^{N-1}|h_n|,\ \max_{0\leqslant i\leqslant N-1}|h_i|\cdot\sum_{n=0}^{N-1}|x_n|\right\}
$$

之最小正整数 t. 则无论用二维或一维的 FNT，其模 $M = 2^{2^t}+1$ 均应满足 $t \geqslant t_0$, 始能保证计算结果的唯一性. 此时易证，当

$$
t_0 \leqslant \begin{cases} \dfrac{m_0-1}{2}\left(或\ \dfrac{m_0-3}{2}\right), & 若\ m_0\ 为奇数, \\ \dfrac{m_0-2}{2}, & 若\ m_0\ 为偶数 \end{cases} \tag{9}
$$

时，可用 α, β 取 2 (或 $\sqrt{2}$)的二维 FNT 计算一维卷积，以缩短用 α 取 2 或 $\sqrt{2}$ 的一维 FNT 计算一维卷积时所需的字长. 事实

上，当用 $\alpha=2$（或$\sqrt{2}$）的一维 FNT 时，若取 $M=2^{2^t}+1$，则必 $t=m_0-1$（或 m_0-2）。由(9)知 $t\geqslant t_0$，此时所需的字长为 2^{m_0-1}（或 2^{m_0-2}）$=\frac{N}{2}\left(或\frac{N}{4}\right)$。而当 m_0 为奇数时，可用 $M=2^{2^t}+1$，$\alpha=\beta=2$（或$\sqrt{2}$），$t=\frac{m_0-1}{2}\left(或\frac{m_0-3}{2}\right)$，$2N_1=N_2=2^{\frac{m_0+1}{2}}$ 的二维 FNT，由(9)知 $t\geqslant t_0$。此时所需的字长为 $2^{\frac{m_0-1}{2}}$（或 $2^{\frac{m_0-3}{2}}$）$=\sqrt{\frac{N}{2}}\left(或\sqrt{\frac{N}{8}}\right)\ll\frac{N}{2}\left(或\frac{N}{4}\right)$。当$m_0$为偶数时，则可用 $M=2^{2^t}+1$，$t=\frac{m_0-2}{2}$，$\alpha=2$，$\beta=\sqrt{2}$，$2N_1=2^{\frac{m_0}{2}}$，$N_2=2^{\frac{m_0}{2}+1}$的二维 FNT，由(9)知 $t\geqslant t_0$。此时所需的字长为 $2^{\frac{m_0-2}{2}}=\sqrt{\frac{N}{4}}\ll\frac{N}{2}\left(或\frac{N}{4}\right)$。

下面给出一个用二维数论变换计算一维循环卷积的例子，因未用快速演段，所以只说明计算的基本概念，而不说明计算的快速效果。

例．求一维序列 $x_0=-1$，$x_1=0$，$x_2=1$，$x_3=-1$，$x_4=0$，$x_5=1$，$x_6=-1$，$x_7=0$；$h_0=h_1=h_2=0$，$h_3=1$，$h_4=h_5=h_6=0$，$h_7=1$ 的循环卷积．

此时 $N=2^3=8$。故若用 $\alpha=2$ 的一维 FNT 来算，则 $t=m_0-1=3-1=2$，即模 $M=2^{2^2}+1=17$，故所需的字长为 4.

今考虑用二维 FNT 来计算，由于

$$\min\left\{\max_{0\leqslant i\leqslant 7}|x_i|\cdot\sum_{n=0}^{7}|h_n|,\right.$$
$$\left.\max_{0\leqslant i\leqslant 7}|h_i|\cdot\sum_{n=0}^{7}|x_n|\right\}=2,$$

故 $t_0=1$。再由 $m_0=3$ 知 $t_0=\frac{m_0-1}{2}$，即(8)式成立．因此可

以断言，此时用 $\alpha=\beta=2$ 之二维 FNT 计算所给的一维卷积必可达到缩短字长的目的。事实上，此时可取 $N_1=2$，$N_2=4$，$\alpha=\beta=2$，$M=2^{2^1}+1=5$，其所需的字长为 2．具体算法是：

先据 (7)，(8)，由所给一维序列作出二维序列

$$\begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \\ x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} \end{pmatrix} = \begin{pmatrix} x_0 & x_2 & x_4 & x_6 \\ x_1 & x_3 & x_5 & x_7 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} h_{0,0} & h_{0,1} & h_{0,2} & h_{0,3} \\ h_{1,0} & h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,0} & h_{2,1} & h_{2,2} & h_{2,3} \\ h_{3,0} & h_{3,1} & h_{3,2} & h_{3,3} \end{pmatrix} = \begin{pmatrix} h_6 & h_0 & h_2 & h_4 \\ h_7 & h_1 & h_3 & h_5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

再写出变换矩阵和其逆阵

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2^2 & 2^3 \\ 1 & 2^2 & 2^4 & 2^6 \\ 1 & 2^3 & 2^6 & 2^9 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix},$$

$$4^{-1}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2^{-1} & 2^{-2} & 2^{-3} \\ 1 & 2^{-2} & 2^{-4} & 2^{-6} \\ 1 & 2^{-3} & 2^{-6} & 2^{-9} \end{pmatrix} = \begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 2 & 1 & -2 \\ -1 & 1 & -1 & 1 \\ -1 & -2 & 1 & 2 \end{pmatrix}.$$

按(4)求出

$$\begin{pmatrix} X_{0,0} & X_{0,1} & X_{0,2} & X_{0,3} \\ X_{1,0} & X_{1,1} & X_{1,2} & X_{1,3} \\ X_{2,0} & X_{2,1} & X_{2,2} & X_{2,3} \\ X_{3,0} & X_{3,1} & X_{3,2} & X_{3,3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix}$$

$$
=\begin{pmatrix} -1 & 0 & 1 & -1 \\ -1 & -1 & 2 & -1 \\ -1 & 2 & -1 & -1 \\ -1 & 3 & -2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix}
$$

$$
=\begin{pmatrix} -1 & 0 & 1 & 1 \\ -1 & 2 & -2 & 2 \\ -1 & 1 & 2 & -1 \\ -1 & -1 & 0 & -2 \end{pmatrix}, \qquad (10)
$$

$$
\begin{pmatrix} H_{0,0} & H_{0,1} & H_{0,2} & H_{0,3} \\ H_{1,0} & H_{1,1} & H_{1,2} & H_{1,3} \\ H_{2,0} & H_{2,1} & H_{2,2} & H_{2,3} \\ H_{3,0} & H_{3,1} & H_{3,2} & H_{3,3} \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}
$$

$$
\times\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix}
$$

$$
=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & -2 & 2 & -2 \\ -1 & -1 & -1 & -1 \\ -2 & 2 & -2 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & 1 & -1 \\ 1 & -2 & -1 & 2 \end{pmatrix}
$$

$$
=\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix}.
$$

再按§6的(5),(6)求

$$
\begin{pmatrix} Y_{0,0} & Y_{0,1} & Y_{0,2} & Y_{0,3} \\ Y_{1,0} & Y_{1,1} & Y_{1,2} & Y_{1,3} \\ Y_{2,0} & Y_{2,1} & Y_{2,2} & Y_{2,3} \\ Y_{3,0} & Y_{3,1} & Y_{3,2} & Y_{3,3} \end{pmatrix}=\begin{pmatrix} X_{0,0}H_{0,0} & X_{0,1}H_{0,1} & X_{0,2}H_{0,2} & X_{0,3}H_{0,3} \\ X_{1,0}H_{1,0} & X_{1,1}H_{1,1} & X_{1,2}H_{1,2} & X_{1,3}H_{1,3} \\ X_{2,0}H_{2,0} & X_{2,1}H_{2,1} & X_{2,2}H_{2,2} & X_{2,3}H_{2,3} \\ X_{3,0}H_{3,0} & X_{3,1}H_{3,1} & X_{3,2}H_{3,2} & X_{3,3}H_{3,3} \end{pmatrix}.
$$

$$
=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},
$$

$$
\begin{pmatrix} y_{0,0} & y_{0,1} & y_{0,2} & y_{0,3} \\ y_{1,0} & y_{1,1} & y_{1,2} & y_{1,3} \\ y_{2,0} & y_{2,1} & y_{2,2} & y_{2,3} \\ y_{3,0} & y_{3,1} & y_{3,2} & y_{3,3} \end{pmatrix} = \begin{pmatrix} y_{0,0} & y_{0,1} & y_{0,2} & y_{0,3} \\ y_{1,0} & y_{1,1} & y_{1,2} & y_{1,3} \\ y_0 & y_2 & y_4 & y_6 \\ y_1 & y_3 & y_5 & y_7 \end{pmatrix}
$$

$$
=\begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 2 & 1 & -2 \\ -1 & 1 & -1 & 1 \\ -1 & -2 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
$$

$$
\times\begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 2 & 1 & -2 \\ -1 & 1 & -1 & 1 \\ -1 & -2 & 1 & 2 \end{pmatrix}
$$

$$
=\begin{pmatrix} 0 & 0 & 1 & 0 \\ -2 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 \\ -2 & 0 & 2 & 0 \end{pmatrix}\begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 2 & 1 & -2 \\ -1 & 1 & -1 & 1 \\ -1 & -2 & 1 & 2 \end{pmatrix}
$$

$$
=\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 1 & -1 & 1 & -1 \\ 0 & -1 & 0 & -1 \end{pmatrix}, \tag{11}
$$

故知所求一维循环卷积是 $y_0=1$, $y_1=0$, $y_2=y_3=-1$, $y_4=1$, $y_5=0$, $y_6=y_7=-1$. 这里 * 表示不必算出的数.

由此例可以看出,计算 (10) 时可节省计算量,计算 (11) 时 * 不必算出,这在一般情形下也是成立的.考虑到上述可节省的计算量,当 $N=N_1\cdot N_2$, $2N_1=N_2$ 时,总的乘加法次数的阶大致为 $5N\log_2 N$.

§8. 多维数论变换

一维与二维数论变换还可以推广到更多维的情况来讨论. 因一般的m维情况($m \geqslant 3$)与二维情况的证明完全类似. 所以下面仅列出其主要定义与结果.

设 $m \geqslant 3$, Z_M 上两个m维序列 $x_{k_1,\cdots,k_m}$ 和 $h_{k_1,\cdots,k_m}$ ($k_i = 0, 1, \cdots, N_i - 1$; $i = 1, \cdots, m$) 的循环卷积是指

$$y_{n_1,\cdots,n_m} = \sum_{k_1=0}^{N_1-1} \cdots \sum_{k_m=0}^{N_m-1} x_{k_1,\cdots,k_m} h_{\langle n_1-k_1\rangle_{N_1},\cdots,\langle n_m-k_m\rangle_{N_m}}$$

$$(n_i = 0, 1, \cdots, N_i - 1;\ i = 1, \cdots, m).$$

设 $x_{i_1,\cdots,i_m} \in Z_M$ ($i_k = 0, 1, \cdots, N_k - 1$; $k = 1, \cdots, m$), 又设 $\alpha_k \in Z_M$ ($k = 1, \cdots, m$), 如果变换

$$X_{k_1,\cdots,k_m} = \sum_{n_1=0}^{N_1-1} \cdots \sum_{n_m=0}^{N_m-1} x_{n_1,\cdots,n_m} \alpha_1^{n_1 k_1} \cdots \alpha_m^{n_m k_m} \tag{1}$$

有循环卷积性质,且有如下形状的逆变换

$$x_{n_1,\cdots,n_m} = N_1^{-1} \cdots N_m^{-1} \sum_{k_1=0}^{N_1-1} \cdots \sum_{k_m=0}^{N_m-1} X_{k_1,\cdots,k_m} \alpha_1^{-n_1 k_1} \cdots \alpha_m^{-n_m k_m},$$

则称(1)为 Z_M 上一个长为 $N_1 \times \cdots \times N_m$ 的m维数论变换.

定理 1. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$, (1)是 Z_M 上一个长为 $N_1 \times \cdots \times N_m$ 的 m 维数论变换的充分必要条件是(1)中的 α_i 是 Z_M 中的 N_i 次单位根,且 α_i 模 p_j 的次数为 N_i ($i = 1, \cdots, m; j = 1, \cdots, s$).

定理 2. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$, (1)是 Z_M 上一个长为 $N_1 \times \cdots \times N_m$ 的m维数论变换的充分必要条件是

$$[N_1, N_2, \cdots, N_m] \mid O(M),$$

这里

$$O(M) = (p_1 - 1, \cdots, p_s - 1).$$

定理 3. 设 $M = p_1^{l_1} \cdots p_s^{l_s}$, 当 $N_1, \cdots, N_m$ 给定后, $[N_1, \cdots, N_m] \mid O(M)$, 则由(1)给出的 Z_M 上的长为 $N_1 \times \cdots \times N_m$ 的m

维数论变换共有 $(\varphi(N_1)\cdots\varphi(N_m))^s$ 个.

下面介绍用三维快速数论变换计算一维卷积.

设 $M = p_1^{l_1}\cdots p_s^{l_s}$, $\alpha_i \in Z_M$, $\alpha_i^{N_i} \equiv 1 \pmod M$, 且 α_i 模 p_j 的次数是 N_i $(i = 1, 2, 3; j = 1, \cdots, s)$, 则

$$X_{k_1,k_2,k_3} = \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\sum_{n_3=0}^{N_3-1} x_{n_1,n_2,n_3}\alpha_1^{n_1k_1}\alpha_2^{n_2k_2}\alpha_3^{n_3k_3} \tag{2}$$

$$(k_i = 0, 1, \cdots, N_i - 1;\ i = 1, 2, 3)$$

给出 Z_M 上一个三维数论变换.

在(2)中, 假设 N_1, N_2, N_3 都是 2 的方幂. 先固定 n_3, 对 $k_1 = 0, 1, \cdots, N_1 - 1$; $k_2 = 0, 1, \cdots, N_2 - 1$ 求出

$$u_{k_1,k_2,n_3} = \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} x_{n_1,n_2,n_3}\alpha_1^{n_1k_1}\alpha_2^{n_2k_2}.$$

由二维的结果知,这共需要 $N_1N_2\log_2 N_1N_2$ 阶次乘、加法运算. 然后变动 $n_3 = 0, 1, \cdots, N_3 - 1$, 知要算出全部 $N_1N_2N_3$ 个 u_{k_1,k_2,k_3} 共需 $N_3N_1N_2\log_2 N_1N_2$ 阶次乘、加法运算. 在此基础上,对固定的 k_1, k_2, 由 $u_{k_1,k_2,0}, \cdots, u_{k_1,k_2,N_3-1}$ 算出 X_{k_1,k_2,k_3}, $k_3 = 0, 1, \cdots, N_3 - 1$, 由一维的结果知, 这需要 $N_3\log_2 N_3$ 阶次乘、加法运算. 而 k_1, k_2 又可取 N_1N_2 组值,故要算出全部 $N_1N_2N_3$ 个 X_{k_1,k_2,k_3} 共需 $N_1N_2N_3\log_2 N_3$ 阶次乘、加法运算. 总起来,要计算出(2)共需

$$N_3N_1N_2\log_2 N_1N_2 + N_1N_2N_3\log_2 N_3 = N_1N_2N_3\log_2 N_1N_2N_3$$

阶次乘、加法运算.

现在讨论用三维数论变换计算一维循环卷积的问题. 设 §7 的(5)中的 $N = 2^m$, $m \geqslant 4$, $N = N_1N_2N_3$, $N_1 \leqslant N_2 \leqslant N_3$, $N_i = 2^{s_i}$, $s_i \geqslant 1$ $(i = 1, 2, 3)$. 据已给的一维序列 x_n, h_n $(n = 0, 1, \cdots, N - 1)$, 作三维序列

$$x_{n_1,n_2,n_3} = \begin{cases} x_{n_1+n_2N_1+n_3N_1N_2} & (n_i = 0, 1, \cdots, N_i - 1;\ i = 1, 2, 3); \\ 0 & (n_1 = N_1, \cdots, 2N_1 - 1;\ n_i = 0, \cdots, N_i - 1;\ i = 2, 3); \end{cases}$$

$$h_{n_1,n_2,n_3} = h_{\langle n_1+(n_2-1)N_1+(n_3-1)N_1N_2\rangle_N}$$

$$(n_1 = 0, 1, \cdots, 2N_1 - 1;\ n_2 = 0, 1, \cdots, 2N_2 - 1;$$
$$n_3 = 0, 1, \cdots, N_3 - 1).$$

今考虑 $n_i=0,1,\cdots,N_i-1\ (i=1,2,3)$ 时，所作出之三维序列的 $N_1N_2N_3=N$ 个部分三维循环卷积

$$\begin{aligned}
y_{N_1+n_1,N_2+n_2,n_3} &= \sum_{k_1=0}^{2N_1-1}\sum_{k_2=0}^{2N_2-1}\sum_{k_3=0}^{N_3-1} x_{k_1,k_2,k_3} h_{\langle N_1+n_1-k_1\rangle_{2N_1},\langle N_2+n_2-k_2\rangle_{2N_2},\langle n_3-k_3\rangle_{N_3}} \\
&= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1}\sum_{k_3=0}^{N_3-1} x_{k_1,k_2,k_3} h_{\langle N_1+n_1-k_1\rangle_{2N_1},\langle N_2+n_2-k_2\rangle_{2N_2},\langle n_3-k_3\rangle_{N_3}} \\
&= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1}\sum_{k_3=0}^{N_3-1} x_{k_1,k_2,k_3} h_{\langle N_1+n_1-k_1+(N_2+n_2-k_2-1)N_1+(n_3-k_3-1)N_1N_2\rangle_N} \\
&= \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1}\sum_{k_3=0}^{N_3-1} x_{k_1+k_2N_1+k_3N_1N_2} h_{\langle n_1+n_2N_1+n_3N_1N_2-(k_1+k_2N_1+k_3N_1N_2)\rangle_N} \\
&= \sum_{k=0}^{N-1} x_k h_{\langle n_1+n_2N_1+n_3N_1N_2-k\rangle_N} \\
&= y_{n_1+n_2N_1+n_3N_1N_2}.
\end{aligned}$$

于是，§7 中（5）的全部值均由此给出。

由本节开头的讨论知，用三维快速数论变换计算一维循环卷积时，可最终地化为一维快速数论变换的计算，且其乘、加法运算次数的阶为 $3\times 4N_1N_2N_3\log_2 4N_1N_2N_3$，即与 $N\log_2 N$ 同阶。对三维快速 FNT 来说，当 $M=2^{2^t}+1=2^b+1$ 给定时，可取 $\alpha_1=\alpha_2=\alpha_3=\sqrt{2}$（或 2），$2N_1=2N_2=N_3=4b$（或 $2b$），其可卷积之一维序列的长度为 $N=N_1N_2N_3=16b^3$（或 $2b^3$）。反之，对给定之一维序列的长度 $N=2^m$，在一定的条件下，用三维快速 FNT 来计算一维卷积时，可使字长从一维快速 FNT 所需的 $\frac{N}{4}\left(\text{或}\ \frac{N}{2}\right)$ 缩短为 $\sqrt[3]{\frac{N}{16}}\left(\text{或}\ \sqrt[3]{\frac{N}{2}}\right)$。

§9. 用孙子定理减少字长

除了用三项式变换和用多维数论变换计算一维卷积可减少字长外，还可用孙子定理来达到这个目的.

设数论变换的参数为 $M=p_1^{l_1}\cdots p_s^{l_s}$, N, α; 整数序列 x_0, x_1, $\cdots$, x_{N-1} 和 h_0, h_1, $\cdots$, h_{N-1} 的循环卷积为

$$y_n=\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\quad (n=0,1,\cdots,N-1). \tag{1}$$

我们来证明

定理. 设 $\alpha_i=\langle\alpha\rangle_{p_i^{l_i}}(i=1,\cdots,s)$, 则参数

$$p_i^{l_i},\ \alpha_i,\ N\ (i=1,\cdots,s) \tag{2}$$

给出 s 个数论变换. 如果用它们计算 (1) 得到[1]

$$\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\equiv y_n^{(i)}\ (\mathrm{mod}\ p_i^{l_i}) \tag{3}$$

$$(n=0,1,\cdots,N-1;\ i=1,\cdots,s).$$

且有

$$y_n\equiv\sum_{i=1}^{s}M_i'M_i y_n^{(i)}\ (\mathrm{mod}\ M)\ \ (n=0,1,\cdots,N-1), \tag{4}$$

其中

$$M=p_i^{l_i}M_i,\quad M_i'M_i\equiv 1\ (\mathrm{mod}\ p_i^{l_i})\quad (i=1,\cdots,s).$$

证. 由于 M, N, α 是一个数论变换的参数，故由§2 定理 1 的条件可以推出 $\alpha_i^N\equiv 1\ (\mathrm{mod}\ p_i^{l_i})$, 且 α_i 对模 p_i 的次数是 $N(i=1,\cdots,s)$. 再由 §2 定理 1 知，(2) 给出 s 个数论变换，故可用它们算出 (3). 而由

$$\sum_{k=0}^{N-1}x_k h_{\langle n-k\rangle_N}\equiv y_n\ (\mathrm{mod}\ M)$$

$(n=0,1,\cdots,N-1)$ 及 (3) 可知

---

1) 这里我们不必假定 $p_i^{l_i}(i=1,\cdots,s)$ 均适合§4 的(2)

$$y_n \equiv y_n^{(i)} \pmod{p_i^{l_i}}$$

$$(i = 0, 1, \cdots, N-1;\ n = 0, 1, \cdots, N-1).$$

于是用孙子定理即得(4). 证完.

由此定理可知，若用参数为 M, N, α 的数论变换计算(1)时所需的机器字长太长，则可用 s 个参数为 $p_i^{l_i}, \alpha_i, N$ $(i=1, \cdots, s)$ 的数论变换(2)求出(3)，然后再用孙子定理求出(4)，而用(2)求(3)时，其模分别是 $p_i^{l_i}$ $(i = 1, \cdots, s)$，而模 $p_i^{l_i}$ 的运算显然比模M的运算所需的字长要少些

第四章 Fermat 数变换实现中的若干问题

在考虑快速数论变换的软件实现时，一则由于通常的数字计算机大多采用二进位计数法，二则由于数论变换中所进行的算术运算是有限环 Z_M 上的算术运算，即模 M 的同余式运算，也即是要求在运算过程中出现大于模 M 的数时必须以其模 M 的最小非负剩余代替它. 因此，要想在计算机上使模M的算术运算得以简化，必须模 M 本身的二进制表示式要尽可能地简单(这显然并不是说 M 必须很小)才行. 在第三章中已知，当 M 为偶数时，数论变换所能卷积之序列的长度 $N = 1$，故无意义. 因此 M 必须取大于 1 的奇数才行，而在大于 1 的奇数中，显然以 Fermat 数 $F_t = 2^b + 1$ $(b = 2^t)$ 之二进制表示式最为简单. 所以，人们在考虑快速数论变换的实现问题时，常只考虑 Fermat 数变换.

§1. 流向图与蝶件

为弄清怎样在计算机上实现快速数论变换，即实现模M的算术运算，我们需要弄清在数论变换的快速演段过程中究竟要用到一些什么样的算术运算.

设已给长为 $N = 2^m$ 的整数序列 $x_0, x_1, \cdots, x_{N-1}$ 和模为M的一个数论变换

$$X_k \equiv \sum_{n=0}^{N-1} x_n \alpha^{nk} \pmod M \qquad (k = 0, 1, \cdots, N-1).$$

计算此变换的快速演段与 FFT 是类似的.

先将足标 n 和 k 表示为二进制数，即设

$$n=\sum_{l=0}^{m-1} n_l 2^l=(n_{m-1}\cdots n_0), \qquad n_l=0 \text{ 或 } 1,$$

$$k=\sum_{q=0}^{m-1} k_q 2^l=(k_{m-1}\cdots k_0), \qquad k_q=0 \text{ 或 } 1.$$

再由 $\alpha^N \equiv 1 \pmod M$，$\alpha^{\frac{N}{2}} \equiv -1 \pmod M$ 可得

$$\begin{aligned}
X_k &= X_{(k_{m-1}\cdots k_0)} \\
&\equiv \sum_{\substack{n_i=0 \\ i=0,1,\cdots,m-1}}^{1} x_{(n_{m-1}\cdots n_0)} \alpha^{\sum_{l=0}^{m-1}\sum_{q=0}^{m-1} n_l k_q 2^{l+q}} \\
&\equiv \sum_{\substack{n_i=0 \\ i=0,1,\cdots,m-1}}^{1} x_{(n_{m-1}\cdots n_0)} \\
&\quad \times \alpha^{\left(\sum\limits_{\substack{0\leqslant l,q\leqslant m-1 \\ l+q\geqslant m}} + \sum\limits_{\substack{0\leqslant l,q\leqslant m-1 \\ l+q=m-1}} + \sum\limits_{\substack{0\leqslant l,q\leqslant m-1 \\ l+q\leqslant m-2}}\right) n_l k_q 2^{l+q}} \\
&\equiv \sum_{\substack{n_i=0 \\ i=0,1,\cdots,m-1}}^{1} x_{(n_{m-1}\cdots n_0)} \cdot (-1)^{\sum_{l=0}^{m-1} n_l k_{m-l-1}} \\
&\quad \times \alpha^{\sum_{q=0}^{m-2}\sum_{l=0}^{m-2-q} k_q n_l 2^{l+q}} \\
&\equiv \sum_{\substack{n_i=0 \\ i=0,1,\cdots,m-2}}^{1} \left\{\left[\sum_{n_{m-1}=0}^{1} x_{(n_{m-1}\cdots n_0)}(-1)^{n_{m-1}k_0}\right]\right. \\
&\quad \left. \times \alpha^{k_0 \sum_{l=0}^{m-2} n_l 2^l}\right\} \cdot (-1)^{\sum_{l=0}^{m-2} n_l k_{m-l-1}} \\
&\quad \times \alpha^{\sum_{q=1}^{m-2}\sum_{l=0}^{m-2-q} k_q n_l 2^{q+l}} \\
&\equiv \sum_{\substack{n_i=0 \\ i=0,1,\cdots,m-2}}^{1} x^{(1)}_{(k_0 n_{m-2}\cdots n_0)} \cdot (-1)^{\sum_{l=0}^{m-2} n_l k_{m-l-1}} \\
&\quad \times \alpha^{\sum_{q=1}^{m-2}\sum_{l=0}^{m-2-q} k_q n_l 2^{q+l}} \\
&\equiv \cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

$$
\begin{aligned}
&\equiv \sum_{\substack{n_i=0\\ i=0,1,\cdots,m-(r+1)}}^{1} x^{(r)}_{(k_0\cdots k_{r-1}n_{m-(r+1)}\cdots n_0)} \\
&\times (-1)^{\sum\limits_{l=0}^{m-(r+1)} n_l k_{m-l-1}} \cdot \alpha^{\sum\limits_{q=r}^{m-2}\sum\limits_{l=0}^{m-2-q} k_q n_l 2^{q+l}} \\
&\equiv \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\equiv \sum_{n_0=0}^{1}\left\{\left[\sum_{n_1=0}^{1} x^{(m-2)}_{(k_0\cdots k_{m-3}n_1n_0)}(-1)^{n_1k_{m-2}}\right]\right. \\
&\qquad \left.\times\ \alpha^{k_{m-2}n_0 2^{m-2}}\right\}(-1)^{n_0k_{m-1}} \\
&\equiv \sum_{n_0=0}^{1} x^{(m-1)}_{(k_0\cdots k_{m-2}n_0)}(-1)^{n_0k_{m-1}} \\
&\equiv x^{(m)}_{(k_0\cdots k_{m-1})} \pmod M, \qquad (1)
\end{aligned}
$$

这里，当 $r=1,2,\cdots,m-1$ 时

$$
x^{(r)}_{(k_0\cdots k_{r-1}n_{m-(r+1)}\cdots n_0)} \equiv \left[\sum_{n_{m-r}=0}^{1} x^{(r-1)}_{(k_0\cdots k_{r-2}n_{m-r}\cdots n_0)}(-1)^{n_{m-r}k_{r-1}}\right] \times \alpha^{k_{r-1}\sum\limits_{l=0}^{m-(r+1)} n_l 2^{l+r-1}} \pmod M.
$$

注意，$\sum\limits_{l=0}^{m-(r+1)} n_l 2^{l+r-1}$ 恰表示 $m-1$ 位的二进制数 $(n_{m-(r+1)}\cdots n_0\overbrace{0\cdots\cdots0}^{r-1\text{个}})$，故上式可更整齐地写作

$$
x^{(r)}_{(k_0\cdots k_{r-1}n_{m-(r+1)}\cdots n_0)} \equiv \left[\sum_{n_{m-r}=0}^{1} x^{(r-1)}_{(k_0\cdots k_{r-2}n_{m-r}\cdots n_0)}(-1)^{n_{m-r}k_{r-1}}\right]\cdot \times\ \alpha^{k_{r-1}(n_{m-(r+1)}\cdots n_0 0\cdots 0)} \pmod M. \qquad (2)
$$

由(1)知，求给定之长为 $N=2^m$ 的序列 $x_0, x_1, \cdots, x_{N-1}$ 的 NTT 值 $X_0, X_1, \cdots, X_{N-1}$ 时，恰可分作 m 次叠代来进行. 但需注意，最后所得的序列 $x^{(m)}_k$ 的足标与欲求值 X_k 的足标恰好是“倒序”相应的，即

$$
X_k = X_{(k_{m-1}\cdots k_0)} \equiv x^{(m)}_{(k_0\cdots k_{m-1})} \pmod M.
$$

下面再看每一次叠代是怎样进行的. 由(2)知，当 $N=2^m$ 个

$x^{(r-1)}_{(k_0\cdots k_{r-2}n_{m-r}\cdots n_0)}$ 已经全部算出而求 $N=2^m$ 个 $x^{(r)}_{(k_0\cdots k_{r-2}k_{r-1}n_{m-r-1}\cdots n_0)}$ 时，对取定的 $k_0, \cdots, k_{r-2}, n_{m-r-1}, \cdots, n_0$（共有 2^{m-1} 组值），$k_{r-1}=0$ 和 1 时的 $x^{(r)}_{(k_0\cdots k_{r-2}k_{r-1}n_{m-r-1}\cdots n_0)}$ 可仅由 $n_{m-r}=0$ 和 1 时的 $x^{(r-1)}_{(k_0\cdots k_{r-2}n_{m-r}n_{m-r-1}\cdots n_0)}$ 来得到，即有

$$\begin{cases} x^{(r)}_{(k_0\cdots k_{r-2}0n_{m-r-1}\cdots n_0)} \equiv x^{(r-1)}_{(k_0\cdots k_{r-2}0n_{m-r-1}\cdots n_0)} \\ \qquad\qquad + x^{(r-1)}_{(k_0\cdots k_{r-2}1n_{m-r-1}\cdots n_0)} \pmod M \\ x^{(r)}_{(k_0\cdots k_{r-2}1n_{m-r-1}\cdots n_0)} \equiv [x^{(r-1)}_{(k_0\cdots k_{r-2}0n_{m-r-1}\cdots n_0)} - x^{(r-1)}_{(k_0\cdots k_{r-2}1n_{m-r-1}\cdots n_0)}] \\ \qquad\qquad \times \alpha^{(n_{m-r-1}\cdots n_0 0\cdots 0)} \pmod M. \end{cases} \tag{3}$$

如果用下面的符号



分别表示 $c \equiv a+b$ 和 $d \equiv (a-b)c \pmod M$，则(3)式可表示为

$x^{(r-1)}_{(k_0\cdots k_{r-2}0n_{m-r-1}\cdots n_0)}$ $x^{(r)}_{(k_0\cdots k_{r-2}0n_{m-r-1}\cdots n_0)}$

$x^{(r-1)}_{(k_0\cdots k_{r-2}1n_{m-r-1}\cdots n_0)}$ $x^{(r)}_{(k_0\cdots k_{r-2}1n_{m-r-1}0\cdots n_0)}$

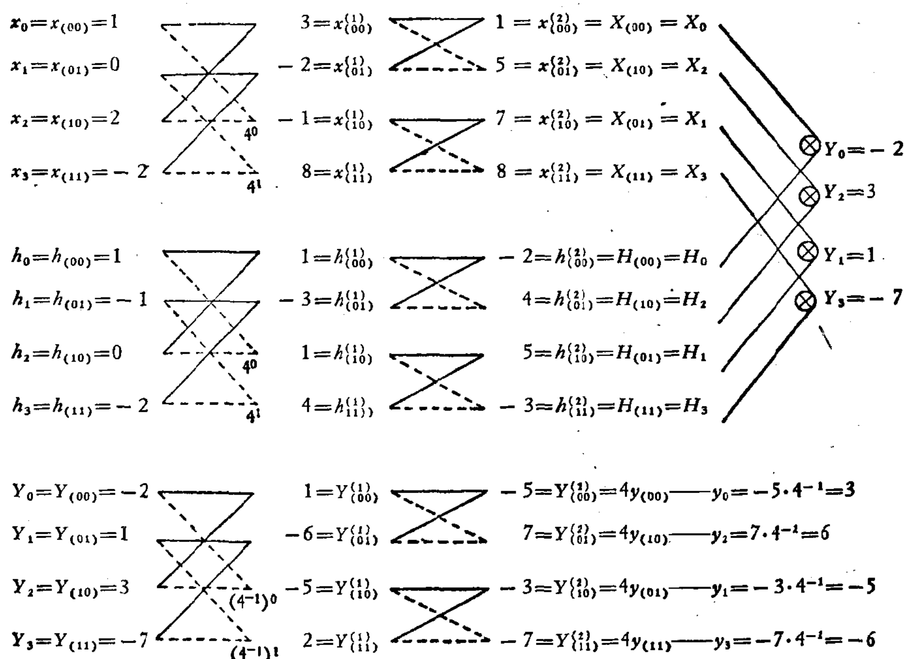
$\alpha^{(n_{m-r-1}\cdots n_0 0\cdots 0)}$.

通常把完成上图所示运算的一个硬件叫做一个蝶件.

由上面的讨论可知，完成一次叠代共需 $2^{m-1}=\frac{N}{2}$ 个蝶件，从而求出整个 NTT 共需 $m\cdot\frac{N}{2}$ 个蝶件. 每个蝶件中需加、减、乘法各一次，故共需加、减法 $2\cdot m\cdot\frac{N}{2}=N\log_2 N$ 次，乘法 $m\cdot\frac{N}{2}=\frac{1}{2}N\log_2 N$ 次. 但因最后由 $x^{(m-1)}_k$ 到 $x^{(m)}_k$ 的叠代中不需乘法，且在第 $r(1\leqslant r\leqslant m-1)$ 次叠代中，对应于 $(k_0,\cdots,k_{r-2},n_{m-r-1},\cdots,n_0)=(k_0,\cdots,k_{r-2},0,\cdots,0)$ 的 2^{r-1} 个蝶件里所乘者均为 $\alpha^0=1$，故亦不需乘法. 而在这 $m-1$ 次叠代中共有 $1+2+2^2+\cdots+2^{m-2}=2^{m-1}-1$ 个这样的蝶件. 故实际上只需乘法 $\frac{1}{2}N\log_2 N-$

$\frac{N}{2}-\left(\frac{N}{2}-1\right)=\frac{1}{2}N(\log_2 N-2)+1$ 次．从上面的讨论还可看出，NTT 的快速演段在大大减少运算次数的同时，并未增加运算的复杂程度，即如 NTT 的定义中那样，仍只需进行两数间的加、减法和乘 α 的方幂的乘法．特别地，当我们只考虑 FNT 时，因常可取 $\alpha=2$，故在其快速演段的实现中只需进行两数间的加、减法和乘 2 的方幂的乘法这三种算术运算就够了．

利用蝶件把 NTT 的快速演段全部表示出，就得到所谓流向图(或流图)．以第三章 § 4 的例子为例，其流向图如下：



符号“⊗”表示相乘．由上图知，就整个求卷积的过程看，共需两次正变换、一次逆变换和 N 次一般乘法．再注意逆变换较正变换多 N 次乘 N^{-1} (它是 2 的方幂)的乘法，便知用快速演段求卷积共需 $3N\log_2 N$ 次加、减法，$\frac{3}{2}N\log_2 N-2N+3$ 次乘 2 的方幂的乘法和 N 次一般乘法

§2. 计算机上模 F_t 运算的实现

由 §1 知道，在计算机上实现 FNT 的快速演段问题归结为在计算机上实现模 F_t 的加、减法和乘 2^k 的问题. 由于减法可通过"取负相加"来实现，故只须考虑模 F_t 的加法、取负和乘 2^k 这三种运算. 但若考虑整个求卷积过程的实现，则还需考虑模 F_t 的一般乘法，下面即将看到，有时是不能如通常那样把一般乘法直接分成几个乘 2^k 的乘法和加法的.

2.1. 普通二进制码 模 $F_t = 2^b + 1 (b = 2^t)$ 的算术运算是限制在整数 $0, 1, \cdots, 2^b - 1, 2^b$ 这 F_t 个数中进行的，即运算中不允许出现大于 2^b 的数. 用一个 b 位寄存器可将 $0, 1, \cdots, 2^b-1$ 全部表示出，但 2^b 这个数却不能表示出. 若只为表示 2^b 这一个数而采用 $b+1$ 位寄存器 (它可表示 $2F_t - 1$ 个数) 又似不大经济，怎么办呢? 由于在实际计算卷积时，b 常取 32 或 64，故若各个数据之间是非相关的，则出现 2^b 这个数的概率大约为 2^{-b}，这是一个很小的数值. 如果一旦出现了 2^b (也就是 -1)这个数，我们就用 0 或 -2 (即 $2^b - 1$) 去代替它，这样作相当于产生了一个偶然的误差. 如果不允许这样的误差，那就只有另外再加一位来表示 2^b. 下面是以 b 位二进制码为基础进行讨论的. 为清楚起见，我们分别用 $\oplus, \ominus, \otimes$ 和 $+, -, \times$ 表示模 F_t 的和普通二进制数的算术运算.

1) 加法

两个 b 位数相加将得到一个 b 位数或 $b+1$ 位数. 在前一种情形，所得的 b 位数就是欲求的和数. 而在后一种情形，因第 $b+1$ 位表示 $2^b \equiv -1 \pmod{F_t}$，故此时模 F_t 的和数应是从所得的 $b+1$ 位数的后 b 位减去 1 后所得的数. 综合起来有

$$A \oplus B = (A + B \text{ 的后 } b \text{ 位}) - (A + B \text{ 的第 } b + 1 \text{ 位}). \quad (1)$$

以 $b = 4$ (即 $F_t = 17$) 为例:

$$
\begin{array}{rr}
10 = & 1\,0\,1\,0 \\
9 = & +\ \ 1\,0\,0\,1 \\
\hline
 & 1\,0\,0\,1\,1 \\
 & -\!\!\longrightarrow 1 \\
\hline
10 \oplus 9 = & 0\,0\,1\,0 = 2,
\end{array}
\qquad
\begin{array}{rr}
5 = & 0\,1\,0\,1 \\
7 = & +\ \ 0\,1\,1\,1 \\
\hline
 & 0\,1\,1\,0\,0 \\
 & -\!\!\longrightarrow 0 \\
\hline
5 \oplus 7 = & 1\,1\,0\,0 = 12.
\end{array}
$$

2) 取负(从而减法)

设 $A = \sum_{i=0}^{b-1} a_i 2^i$，$a_i = 0$ 或 1，又设 $\bar{a}_i$ 表示 a_i 的补，即 $a_i + \bar{a}_i = 1$，$\bar{A} = \sum_{i=0}^{b-1} \bar{a}_i 2^i$ 表示 A 的补．则

$$
\begin{aligned}
-A &= -\sum_{i=0}^{b-1} a_i 2^i = \sum_{i=0}^{b-1} (\bar{a}_i - 1) = \sum_{i=0}^{b-1} \bar{a}_i - (2^b - 1) \\
&\equiv \bar{A} + 2 \pmod{F_t}.
\end{aligned}
$$

故有

$$
\ominus A = \bar{A} \oplus 2, \tag{2}
$$

即一数模 F_t 的负数等于该数的补与 2 模 F_t 的和数.

例. $b = 4$ 时

$$
\begin{array}{rr}
\bar{7} = & \bar{0}\,\bar{1}\,\bar{1}\,\bar{1} \\
2 = & +\ \ 0\,0\,1\,0 \\
\hline
 & 0\,1\,0\,1\,0 \\
 & -\!\!\longrightarrow 0 \\
\hline
\ominus 7 = & 1\,0\,1\,0 = 10
\end{array}
\qquad
\begin{array}{rr}
\bar{0} = & \bar{0}\,\bar{0}\,\bar{0}\,\bar{0} \\
2 = & +\ \ 0\,0\,1\,0 \\
\hline
 & 1\,0\,0\,0\,1 \\
 & -\!\!\longrightarrow 1 \\
\hline
\ominus 0 = & 0\,0\,0\,0 = 0
\end{array}
$$

$$
\begin{aligned}
10 \ominus 7 &= 10 \oplus (\ominus 7) \\
&= 10 \oplus 10 \\
&= 3
\end{aligned}
\qquad
\begin{array}{rr}
 & 1\,0\,1\,0 \\
+ & 1\,0\,1\,0 \\
\hline
 & 1\,0\,1\,0\,0 \\
 & -\!\!\longrightarrow 1 \\
\hline
 & 0\,0\,1\,1 = 3.
\end{array}
$$

3) 乘 2^k 的乘法

因 $2^b \equiv -1 \pmod{F_t}$，故可设 $0 < k < b$. 则

$$
2^k A = 2^k \sum_{i=0}^{b-1} a_i 2^i
$$

$$= 2^b(a_{b-1}2^{k-1}+\cdots+a_{b-k})+a_{b-k-1}2^{b-1}+\cdots+a_02^k$$

$$\equiv a_{b-k-1}2^{b-1}+\cdots+a_02^k-(a_{b-1}2^{k-1}+\cdots+a_{b-k}) \pmod{F_t}.$$

这说明

$$2^k\otimes A=(\text{将}A\text{左移}k\text{位后所得的}b\text{位数})\ominus(\text{移出所得的}k\text{位数}). \tag{3}$$

例. $b=4$ 时

11 = 1011，左移 3 位后所得的 4 位数为 1000，而移出的 3 位数为 101 = 0101，其负数为 1100. 故知

$$2^3\otimes 11=3,$$

```
    1 0 0 0
+   1 1 0 0
-----------
  1 0 1 0 0
-  ⌣⌣⌣⌣→1
-----------
    0 0 1 1 = 3.
```

在计算逆变换时需乘 2^{-k}. 因 $2^{-k}\equiv -2^{b-k}\pmod{F_t}$，故

$$2^{-k}\otimes A=\ominus 2^{b-k}\otimes A=2^{b-k}\otimes(\ominus A). \tag{4}$$

例. $b=4$ 时

$\ominus 7=1010$，左移 2 位得 1000，移出数 0010 取负为 1111，故知

$$2^{-2}\otimes 7=2^2\otimes(\ominus 7)=6,$$

```
    1 0 0 0
+   1 1 1 1
-----------
  1 0 1 1 1
-  ⌣⌣⌣⌣→1
-----------
    0 1 1 0 = 6.
```

4）一般乘法

一般乘法原则上可通过先作若干个乘 2^k 的乘法和加法来实现. 但也可直接作如下的考虑. 因两个 b 位数相乘之积是一个 $2b$ 位数，若以 C_H 和 C_L 分别表示 $2b$ 位数 $A\times B$ 的高 b 位和低 b 位所得的 b 位数，则

$$A\times B=2^bC_H+C_L\equiv C_L-C_H\pmod{F_t},$$

故

$$A\otimes B=C_L\ominus C_H$$
$$=(A\times B\text{的低}b\text{位})\ominus(A\times B\text{的高}b\text{位}). \tag{5}$$

例. $b=4$ 时

$$
\begin{array}{rr}
13 = & 1\,1\,0\,1 \\
9 = \times & 1\,0\,0\,1 \\
\hline
 & 1\,1\,0\,1 \\
 1\,1\,0\,1 & \\
\hline
13\times 9 = & \underbrace{0\,1\,1\,1}_{C_H}\ \underbrace{0\,1\,0\,1}_{C_L}
\end{array}
\qquad
\begin{array}{rr}
C_L = & 0\,1\,0\,1 \\
\ominus C_H = + & 1\,0\,1\,0 \\
\hline
 & 0\,1\,1\,1\,1 \\
 & -\!\!\longrightarrow 0 \\
\hline
13 \otimes 9 = & 1\,1\,1\,1 = 15.
\end{array}
$$

2.2. 新码 上节讨论普通二进制码的模 F_t 运算时，为简化运算而把运算限制在 b 位码上进行. 这样，由于 2^b(即-1)这个数不能用 b 位表示出，故凡运算结果是2^b时(例如在加法中当$A\oplus B=2^b$时、取负中 $A=1$ 时)或参与运算的两数中有一个是 2^b 时，所述模 F_t 的运算均不能进行. 如果采用以 0 或 2^b-1 (即 -2) 代替 2^b 的办法，误差的积累有时将大大影响最后所得计算结果的精度. 就是把运算扩大到 $b+1$ 位进行，在实现 $2^b\otimes 2^b=1$，即 $10\cdots 0\otimes 10\cdots 0=0\cdots 01$ 时，仍是十分困难的! 因此，用普通二进制码进行模 F_t 运算时，本质的困难在于 2^b 这个数的表现形式(即 $10\cdots 0$)和它的具体内容(即 2^b 起作 -1 的作用)之间的矛盾. 为了解决这一矛盾，达到精确地计算 FNT 的目的，人们引入了 0 到 2^b 这 F_t 个数的一种新的表示方法——新码. 在新码中，原来表示 $2^{b-1}-1$ 的普通二进制码 $0\ 0\ \overbrace{1\ 1\ \cdots\ 1}^{b-1\text{个}}$ 被用来表示 2^b 这个数，而原来表 2^b 的普通二进制码 $1\ \overbrace{0\ \cdots\ 0}^{b\text{个}}$ 则被用来表示数 0. 这样一来，由于 0 这个数与任何数相加、相乘的结果都是十分显然的，因此在新码中就巧妙地避开了对数码 $1\ \overbrace{0\ \cdots\ 0}^{b\text{个}}$ 进行运算，从而达到了精确计算 FNT 的目的. 而且从下面的讨论中还可看到，用新码作模 F_t 的运算时，与用普通二进制码相比，其运算规则反而还要更加简便一些.

新的表示数方法是这样的: 因对任意整数 B，$B\in Z_{F_t}=\{0, 1, \cdots, 2^b\}$，$b=2^t$，均可找到唯一的整数 $\hat{B}\in Z_{F_t}$，适合条件

$$B\equiv 2\hat{B}+2\ (\mathrm{mod}\ F_t), \tag{1}$$

且反之亦真．我们就用 $\hat{B}$ 的普通 $b+1$ 位二进制码作为 B 的新码．以 $b=4$ 为例，此时 $F_2=2^{2^2}+1=17$．若 $B=0$，则因 $0\equiv 2\cdot 2^4+2\ (\mathrm{mod}\ 17)$，故 0 的新码就是 2^4 的旧码（即普通二进制码）1 0 0 0 0；若 $B=2^4$，则因 $2^4\equiv 2\cdot(2^3-1)+2\ (\mathrm{mod}\ 17)$，故 2^4 的新码就是 2^3-1 的旧码 0 0 1 1 1；若 $B=9$，则因 $9\equiv 2\cdot 12+2\ (\mathrm{mod}\ 17)$，故 9 的新码就是 12 的旧码 0 1 1 0 0；等等．显然，当 $b=2^t$ 较大时，从定义 (1) 出发先求 $\hat{B}$ 再求 B 的新码的办法是十分麻烦的．能否直接从 B 的旧码（B 给定后是很容易知道的）出发来导出 B 的新码呢？可以的．

由 (1) 知，当 $B=0$ 和 2^b 时，$\hat{B}=2^b$ 和 $2^{b-1}-1$，故其新码分别为 $1\,\overbrace{0\ \cdots\ 0}^{b\text{个}}$ 和 $0\ 0\,\overbrace{1\ 1\ \cdots\ 1}^{b-1\text{个}}$．

当 $B\neq 0$ 和 2^b 时，可设

$B=0\cdot 2^b+e_{b-1}2^{b-1}+\cdots+e_1\cdot 2^1+e_0$，$e_i$ 不全为 0．因 $2^{-1}\equiv 2^{b-1}+1\ (\mathrm{mod}\ 2^b+1)$，故由 (1) 知

$$\hat{B}\equiv 2^{-1}B-1\equiv 2^{b-1}B+B-1\ (\mathrm{mod}\ 2^b+1).$$

由于

$$\begin{aligned}2^{b-1}B&=2^b(e_{b-1}2^{b-2}+\cdots+e_1)+e_0 2^{b-1}\\&\equiv e_0 2^{b-1}-(e_{b-1}2^{b-2}+\cdots+e_1)\ (\mathrm{mod}\ 2^b+1),\\B&=2(e_{b-1}2^{b-2}+\cdots+e_1)+e_0,\end{aligned}$$

故

$$\hat{B}\equiv e_0 2^{b-1}+(e_{b-1}2^{b-2}+\cdots+e_1)-\bar{e}_0\ (\mathrm{mod}\ 2^b+1).$$

因 e_i 不全为 0，上式右边之值恒在 0 与 2^b 之间，再由 $\hat{B}\in Z_{F_t}$ 知

$$\hat{B}=0\cdot 2^b+e_0 2^{b-1}+e_{b-1}2^{b-2}+\cdots+e_1-\bar{e}_0. \tag{2}$$

(2)式说明，除 $B=0$ 和 2^b 这两个极端值外，B 之新码可由其旧码的后 b 位由尾向前循环移动一位后再减去（普通二进制减法）第 b 位之补而得到．反之，若已知 B 之新码，则其旧码可由新码加上（普通二进制加法）第 b 位之补后再将后 b 位由前向尾循环移动一位而得到．

例．$b=4$ 时

$$
\begin{array}{l}
B = 6 = 0\,0\,1\,1\,0 \rightarrow \quad 0\,0\,0\,1\,1 \\
\qquad\qquad\qquad\qquad\quad - \longrightarrow \bar{0} \\
\hline
\qquad\qquad\qquad\qquad\quad 0\,0\,0\,1\,0 = 2 = \hat{B};
\end{array}
$$

$$
\begin{array}{l}
\hat{B} = 2 = \quad 0\,0\,0\,1\,0 \\
\qquad + \longrightarrow \bar{0} \\
\hline
\qquad\quad 0\,0\,0\,1\,1 \rightarrow 0\,0\,1\,1\,0 = 6 = B.
\end{array}
$$

据此就可很快地算出 0 到 $2^b = 2^4 = 16$ 各数的新码如下：

表 1.　$b = 4$ 时新、旧码对照表

正规值 (B)	旧　码 (B 的二进制码)	新　码 ($\hat{B}$ 的二进制码)	对应值 ($\hat{B}$)
0	0 0 0 0 0	1 0 0 0 0	16
1	0 0 0 0 1	0 1 0 0 0	8
2	0 0 0 1 0	0 0 0 0 0	0
3	0 0 0 1 1	0 1 0 0 1	9
4	0 0 1 0 0	0 0 0 0 1	1
5	0 0 1 0 1	0 1 0 1 0	10
6	0 0 1 1 0	0 0 0 1 0	2
7	0 0 1 1 1	0 1 0 1 1	11
8	0 1 0 0 0	0 0 0 1 1	3
9 (−8)	0 1 0 0 1	0 1 1 0 0	12
10 (−7)	0 1 0 1 0	0 0 1 0 0	4
11 (−6)	0 1 0 1 1	0 1 1 0 1	13
12 (−5)	0 1 1 0 0	0 0 1 0 1	5
13 (−4)	0 1 1 0 1	0 1 1 1 0	14
14 (−3)	0 1 1 1 0	0 0 1 1 0	6
15 (−2)	0 1 1 1 1	0 1 1 1 1	15
16 (−1)	1 0 0 0 0	0 0 1 1 1	7

下面讨论新码模 $2^b + 1$ 运算的规则. 显然，这些规则必须满足二数新码的和、差、积恰好就是该二数和、差、积的新码，即若以符号 $\widehat{\oplus}$、$\widehat{\ominus}$、$\widehat{\otimes}$ 表新码间的加、减、乘法规则，就应有

$$\hat{A} \,\widehat{\oplus}\, \hat{B} = \widehat{A \oplus B}, \quad \widehat{\ominus}\, \hat{A} = \widehat{\ominus A}, \quad \hat{A} \,\widehat{\oplus}\, \hat{B} = \widehat{A \otimes B}.$$

1) 加法

设

$$A \equiv 2\hat{A} + 2, \quad B \equiv 2\hat{B} + 2 \pmod{2^b + 1},$$

则

$$A \oplus B \equiv A + B \equiv 2(\hat{A} + \hat{B} + 1) + 2 \pmod{2^b + 1}.$$

故有

$$\hat{A} \widehat{\oplus} \hat{B} = \widehat{A \oplus B} \equiv \hat{A} + \hat{B} + 1 \pmod{2^b + 1}. \qquad (3)_1$$

当 A, B 之一,例如 A 为 0 时, $\hat{A} = 2^b$, 由$(3)_1$知 $\hat{A} \widehat{\oplus} \hat{B} = \hat{B}$. 故在新码的运算中,上小节难以处理的数码 1 0 ··· 0, 现在可以看作一个停止运算进行的禁止信号,而不参加运算.

当 A, B 均不为 0 时, $\hat{A}$, $\hat{B}$ 均不为 2^b, 故可设

$$\hat{A} + \hat{B} = c_b 2^b + c_{b-1} 2^{b-1} + \cdots + c_0.$$

从而由$(3)_1$知

$$\hat{A} \widehat{\oplus} \hat{B} \equiv \hat{A} + \hat{B} + 1 \equiv 0 \cdot 2^b + c_{b-1} 2^{b-1} + \cdots + c_0 + 1 - c_b$$
$$\equiv 0 \cdot 2^b + c_{b-1} 2^{b-1} + \cdots + c_0 + \bar{c}_b \pmod{2^b + 1},$$

因上式两端之值均在 0 到 2^b 之间,故得

$$\hat{A} \widehat{\oplus} \hat{B} = 0 \cdot 2^b + c_{b-1} 2^{b-1} + \cdots + c_0 + \bar{c}_b$$
$$= (\hat{A} + \hat{B} \text{ 的后 } b \text{ 位}) + (\hat{A} + \hat{B} \text{ 的第 } b + 1 \text{ 位之补}). \qquad (3)_2$$

例如 $b = 4$ 时:

$$\begin{array}{rr}
\hat{5} = 10 = & 0\ 1\ 0\ 1\ 0 \\
\hat{5} = 10 = & +\ 0\ 1\ 0\ 1\ 0 \\
\hline
 & 1\ 0\ 1\ 0\ 0 \\
 & + \longrightarrow \bar{1} \\
\hline
\hat{5} \widehat{\oplus} \hat{5} = & 0\ 0\ 1\ 0\ 0 \ = 4 = \widehat{10},
\end{array}$$

$$\begin{array}{rr}
\widehat{12} = 5 = & 0\ 0\ 1\ 0\ 1 \\
\hat{8} = 3 = & +\ 0\ 0\ 0\ 1\ 1 \\
\hline
 & 0\ 1\ 0\ 0\ 0 \\
 & + \longrightarrow \bar{0} \\
\hline
\widehat{12} \widehat{\oplus} \hat{8} = & 0\ 1\ 0\ 0\ 1 \ = 9 = \hat{3}.
\end{array}$$

2) 取负(从而减法)

设

$$B \equiv 2\hat{B} + 2 \pmod{2^b + 1},$$

则

$$\ominus B \equiv -B \equiv 2(-\hat{B}-2)+2 \pmod{2^b+1},$$

故

$$\widehat{\ominus}\,\hat{B} = \widehat{\ominus B} \equiv -\hat{B}-2 \pmod{2^b+1}. \tag{4}_1$$

若 $B=0$, 即 $\hat{B}=1\overbrace{0\cdots0}^{b\text{个}}$, 则

$$\widehat{\ominus}\,\hat{B} \equiv -2^b-2 \equiv 1-2 \equiv -1 \equiv 2^b \equiv \hat{B} \pmod{2^b+1},$$

从而 $\widehat{\ominus}\,\hat{B}=\hat{B}$. 故如 1) 那样, $1\ 0\cdots0$ 的出现仍可看作停止运算进行的禁止信号.

若 $B \neq 0$, 即 $\hat{B} \neq 2^b$, 则可设

$$\hat{B} = 0\cdot2^b + e_{b-1}2^{b-1}+\cdots+e_0.$$

于是由 $(4)_1$ 知

$$\begin{aligned}
\widehat{\ominus}\,\hat{B} &\equiv -\hat{B}-2 \equiv 0\cdot2^b - e_{b-1}2^{b-1}-\cdots-e_0-2\\
&\equiv 0\cdot2^b - e_{b-1}2^{b-1}-\cdots-e_0+2^b-1\\
&\equiv 0\cdot2^b+(1-e_{b-1})2^{b-1}+\cdots+(1-e_0)\\
&\equiv 0\cdot2^b+\bar{e}_{b-1}2^{b-1}+\cdots+\bar{e}_0 \pmod{2^b+1}.
\end{aligned}$$

同样,因上式两端之值均在 0 到 2^b 之间,故有

$$\begin{aligned}
\widehat{\ominus}\,\hat{B} &= 0\cdot2^b+\bar{e}_{b-1}2^{b-1}+\cdots+\bar{e}_0\\
&= (\text{对 } \hat{B} \text{ 之后 } b \text{ 位取补}).
\end{aligned} \tag{4}_2$$

例如 $b=4$ 时, $\hat{5}=0\ 1\ 0\ 1\ 0$, 故 $\widehat{\ominus}\,\hat{5}=0\bar{1}\ \bar{0}\ \bar{1}\ \bar{0}=0\ 0\ 1\ 0\ 1$ $=5=\widehat{12}=\widehat{\ominus5}$.

3) 乘 2^k 的乘法

不失一般性,可设 $0<k<b$. 且设

$$B \equiv 2\hat{B}+2 \pmod{2^b+1}.$$

则

$$\begin{aligned}
2^k \otimes B &\equiv 2^k \times B \equiv 2^k\times(2\hat{B}+2)\\
&\equiv 2(2^k\times\hat{B}+2^k-1)+2 \pmod{2^b+1}.
\end{aligned}$$

故

$$\widehat{2^k}\,\widehat{\otimes}\,\hat{B} = \widehat{2^k\otimes B} \equiv 2^k\times\hat{B}+2^k-1 \pmod{2^b+1}. \tag{5}_1$$

若 $B=0$, 即 $\hat{B}=2^b$, 则

$$\widehat{2^k}\otimes \hat{B} \equiv 2^k \times 2^b + 2^k - 1 \equiv 2^k(2^b+1) - 1 \equiv -1$$
$$\equiv 2^b \pmod{2^b+1}.$$

从而 $\widehat{2^k}\otimes \hat{B} = \hat{B}$，故仍可将 1 0 ··· 0 作为禁止信号来看待

若 $B \neq 0$，即 $\hat{B} \neq 2^b$，故可设

$$\hat{B} = 0\cdot 2^b + e_{b-1}2^{b-1} + \cdots + e_0.$$

于是由 $(5)_1$ 知

$$\begin{aligned}\widehat{2^k}\otimes \hat{B} &\equiv 2^k \times \hat{B} + 2^k - 1\\ &\equiv 0\cdot 2^{b+k} + e_{b-1}2^{b+k-1} + \cdots + e_{b-1-k}2^{b-1} + \cdots\\ &\qquad + e_0 2^k + 2^k - 1\\ &\equiv 0\cdot 2^b + e_{b-1-k}2^{b-1} + \cdots + e_0 2^k\\ &\qquad - e_{b-1}2^{k-1} - \cdots - e_{b-k} + 2^k - 1\\ &\equiv 0\cdot 2^b + e_{b-1-k}2^{b-1} + \cdots + e_0 2^k + \bar{e}_{b-1}2^{k-1} + \cdots\\ &\qquad + \bar{e}_{b-k} \pmod{2^b+1}.\end{aligned}$$

上式两端之值均在 0 到 2^b 之间，故得

$$\widehat{2^k}\otimes \hat{B} = 0\cdot 2^b + e_{b-1-k}2^{b-1} + \cdots + e_0 2^k + \bar{e}_{b-1}2^{k-1} + \cdots + \bar{e}_{b-k}$$

=（将 $\hat{B}$ 的后 b 位自前向后循环移动 k 位，再取最后 k 位之补）。 $(5)_2$

例如 $b = 4$ 时：

$\hat{5} = 0\ 1\ 0\ 1\ 0 \to 0\ 0\ 1\ 0\ 1 \to 0\ 1\ 0\ 1\ 0 \to 0\ 0\ 1\ 0\ 1$,

故知 $\widehat{2^3}\otimes \hat{5} = 0\ 0\ \bar{1}\ \bar{0}\ \bar{1} = 0\ 0\ 0\ 1\ 0 = 2 = \hat{6}$;

$\hat{7} = 0\ 1\ 0\ 1\ 1 \to 0\ 0\ 1\ 1\ 1 \to 0\ 1\ 1\ 1\ 0$，故知 $\hat{2}^2 \otimes \hat{7} = 0\ 1\ 1\ \bar{1}\ \bar{0} = 0\ 1\ 1\ 0\ 1 = 13 = \widehat{11}$.

4）一般乘法

设

$$A \equiv 2\hat{A} + 2,\quad B \equiv 2\hat{B} + 2 \pmod{2^b+1},$$

则

$$\begin{aligned}A\otimes B &\equiv A \times B \equiv (2\hat{A}+2)(2\hat{B}+2)\\ &\equiv 2[2(\hat{A}\times\hat{B} + \hat{A} + \hat{B}) + 1] + 2 \pmod{2^b+1}.\end{aligned}$$

故

$$\hat{A}\widehat{\otimes}\hat{B}=\widehat{A\otimes B}\equiv 2(\hat{A}\times\hat{B}+\hat{A}+\hat{B})+1\ (\mathrm{mod}\ 2^b+1).\quad (6)_1$$

若 A, B 中有一为0,即 $\hat{A}$, $\hat{B}$ 中有一为 2^b(例如 $\hat{A}=2^b$), 则由 $(6)_1$ 知

$$\begin{aligned}\hat{A}\widehat{\otimes}\hat{B}&\equiv 2(2^b\times\hat{B}+2^b+\hat{B})+1\\&\equiv 2(-\hat{B}+2^b+\hat{B})+1\\&\equiv 2^{b+1}+1\equiv 2^b+2^b+1\equiv 2^b\\&\equiv\hat{A}\ (\mathrm{mod}\ 2^b+1),\end{aligned}$$

故新码中出现 1 0 $\cdots$ 0 时,运算不需进行,其积就是 1 0 $\cdots$ 0.

若 A, B 均不为 0, 即 $\hat{A}$, $\hat{B}$ 均不为 2^b. 写

$$\hat{A}=\sum_{k=0}^{b-1}a_k2^k(a_k=0\text{ 或 }1),$$

则由 $(5)_1$ 知

$$\begin{aligned}\hat{A}\times\hat{B}&=\sum_{k=0}^{b-1}(a_k2^k\times\hat{B})\\&=\sum_{k=0}^{b-1}(a_k2^k\times\hat{B}+2^{ka_k}-1)-\sum_{k=0}^{b-1}(2^{ka_k}-1)\\&\equiv\sum_{k=0}^{b-1}[(\widehat{a_k2^k})\widehat{\otimes}\hat{B}]-\sum_{k=0}^{b-1}a_k2^k+r\ \ (\mathrm{mod}\ 2^b+1),\end{aligned}$$

这里, r 表示非零的 a_k 之个数.

记

$$\widehat{\oplus}_{k=1}^{m}\hat{A}_k=\hat{A}_1\widehat{\oplus}\hat{A}_2\widehat{\oplus}\cdots\widehat{\oplus}\hat{A}_m,$$

则由 $(3)_1$ 知

$$\widehat{\oplus}_{k=1}^{m}\hat{A}_k\equiv\sum_{k=1}^{m}\hat{A}_k+m-1\ (\mathrm{mod}\ 2^b+1).$$

于是

$$\hat{A}\times\hat{B}\equiv\widehat{\oplus}_{k=0}^{b-1}[(\widehat{a_k2^k})\widehat{\otimes}\hat{B}]-\hat{A}+1\ (\mathrm{mod}\ 2^b+1).$$

再由 $(3)_1$, $(5)_1$ 和 $(6)_1$ 得

$$\begin{aligned}\hat{A}\widehat{\otimes}\hat{B}&\equiv\hat{2}\widehat{\otimes}(\hat{A}\times\hat{B}+\hat{A}+\hat{B})\\&\equiv\hat{2}\widehat{\otimes}\{\widehat{\oplus}_{k=0}^{b-1}[(\widehat{a_k2^k})\widehat{\otimes}\hat{B}]+\hat{B}+1\}\end{aligned}$$

$$\equiv \hat{2}\,\widehat{\otimes}\,\{(\widehat{\oplus}_{k=0}^{b-1}[(\widehat{a_k 2^k})\,\widehat{\otimes}\,\hat{B}])\,\widehat{\oplus}\,\hat{B}\}\ (\bmod 2^b+1).$$

由于上式右边均为新码的模 2^b+1 运算，最后算出之值应在 0 到 2^b 之间，故有

$$\hat{A}\,\widehat{\otimes}\,\hat{B} = \hat{2}\,\widehat{\otimes}\,\{(\widehat{\oplus}_{k=0}^{b-1}[(\widehat{a_k 2^k})\,\widehat{\otimes}\,\hat{B}])\,\widehat{\oplus}\,\hat{B}\}. \qquad (6)_2$$

$(6)_2$ 看起来复杂，实际上仍是比较方便的，例如 $b=4$ 时：

$\hat{A}=\widehat{14}=0\ 0\ 1\ 1\ 0$,	$\hat{A}=\widehat{12}=0\ 0\ 1\ 0\ 1$,
$\hat{B}=\widehat{11}=0\ 1\ 1\ 0\ 1$,	$\hat{B}=\hat{9}=0\ 1\ 1\ 0\ 0$,
$\hat{A}$ 的二进制表示式中只有 a_1, a_2 不为 0.	$\hat{A}$ 的二进制表示式中只有 a_0, a_2 不为 0.
$\hat{2}^1\widehat{\otimes}\hat{B}=\ 0\ 1\ 0\ 1\ 0$	$\hat{2}^0\widehat{\otimes}\hat{B}=\ 0\ 1\ 1\ 0\ 0$
$\hat{2}^2\widehat{\otimes}\hat{B}=\ +\ 0\ 0\ 1\ 0\ 0$	$\hat{2}^2\widehat{\otimes}\hat{B}=\ +\ 0\ 0\ 0\ 0\ 0$
$0\ 1\ 1\ 1\ 0$	$0\ 1\ 1\ 0\ 0$
$\widehat{\oplus}_{k=1}^{2}(\hat{2}^k\widehat{\otimes}\hat{B})=\ + \rightarrow \bar{0}$	$\widehat{\oplus}_{k=0,2}(\hat{2}^k\widehat{\otimes}\hat{B})=\ + \rightarrow \bar{0}$
$0\ 1\ 1\ 1\ 1$	$0\ 1\ 1\ 0\ 1$
$\hat{B}=\ +\ 0\ 1\ 1\ 0\ 1$	$\hat{B}=\ +\ 0\ 1\ 1\ 0\ 0$
$1\ 1\ 1\ 0\ 0$	$1\ 1\ 0\ 0\ 1$
$\widehat{\oplus}_{k=1}^{2}(\hat{2}^k\widehat{\otimes}\hat{B})\widehat{\oplus}\hat{B}=\ + \rightarrow \bar{1}$	$\widehat{\oplus}_{k=0,2}(\hat{2}^k\widehat{\otimes}\hat{B})\widehat{\oplus}\hat{B}=\ + \rightarrow \bar{1}$
$0\ 1\ 1\ 0\ 0$	$0\ 1\ 0\ 0\ 1$
再 $\widehat{\otimes}\hat{2}=\ 0\ 1\ 0\ 0\ 0=\hat{1}$	再 $\widehat{\otimes}\hat{2}=\ 0\ 0\ 0\ 1\ 0=\hat{6}$
故知 $\widehat{14}\,\widehat{\otimes}\,\widehat{11}=\hat{1}$.	故知 $\widehat{12}\,\widehat{\otimes}\,\hat{9}=\hat{6}$.

值得注意的是，当我们不用 A 的新码而用 A 的旧码时，运算规则将比较简单. 设 $A=\sum_{k=0}^{b-1} e_k 2^k$，则

$$A\otimes B\equiv A\times B\equiv\sum_{k=0}^{b-1}(e_k 2^k\times B)$$
$$\equiv \oplus_{k=0}^{b-1}(e_k 2^k\otimes B)\ (\bmod 2^b+1),$$

由于上式两边之值均在 0 到 2^b 间，故有

$$A\otimes B=\oplus_{k=0}^{b-1}(e_k 2^k\otimes B).$$

于是由定义知

$$\hat{A}\,\widehat{\otimes}\,\hat{B}=\widehat{A\otimes B}=\widehat{\oplus_{k=0}^{b-1}(e_k 2^k\otimes B)}=\widehat{\oplus}_{k=0}^{b-1}[\widehat{e_k 2^k\otimes B}]$$
$$=\widehat{\oplus}_{k=0}^{b-1}[(\widehat{e_k 2^k})\,\widehat{\otimes}\,\hat{B}]. \qquad (6)_3$$

例如在上面的例子中：

$$
\begin{array}{rl}
A = 14 = & 0\ 1\ 1\ 1\ 0, \\
\hat{B} = \widehat{11} = & 0\ 1\ 1\ 0\ 1, \\
\hat{2}^1 \widehat{\otimes} \hat{B} = & \ \ 0\ 1\ 0\ 1\ 0 \\
\hat{2}^2 \widehat{\otimes} \hat{B} = & \underline{+\ 0\ 0\ 1\ 0\ 0} \\
 & \ \ 0\ 1\ 1\ 1\ 0 \\
\widehat{\oplus}_{k=1}^{2} (\hat{2}^k \widehat{\otimes} \hat{B}) = & \underline{+ \longrightarrow \bar{0}} \\
 & \ \ 0\ 1\ 1\ 1\ 1 \\
\hat{2}^3 \widehat{\otimes} \hat{B} = & \underline{+\ 0\ 1\ 0\ 0\ 1} \\
 & \ \ 1\ 1\ 0\ 0\ 0 \\
\widehat{14} \widehat{\otimes} \widehat{11} = & \underline{+ \longrightarrow \bar{1}} \\
 & \ \ 0\ 1\ 0\ 0\ 0 = 1.
\end{array}
\qquad\Bigg|\qquad
\begin{array}{rl}
A = 12 = & 0\ 1\ 1\ 0\ 0, \\
\hat{B} = \hat{9} = & 0\ 1\ 1\ 0\ 0, \\
\hat{2}^2 \widehat{\otimes} \hat{B} = & \ \ 0\ 0\ 0\ 0\ 0 \\
\hat{2}^3 \widehat{\otimes} \hat{B} = & \underline{+\ 0\ 0\ 0\ 0\ 1} \\
 & \ \ 0\ 0\ 0\ 0\ 1 \\
\widehat{12} \widehat{\otimes} \hat{9} = & \underline{+ \longrightarrow \bar{0}} \\
 & \ \ 0\ 0\ 0\ 1\ 0 = \hat{6}.
\end{array}
$$

虽然用 $(6)_3$ 作一般乘法比用 $(6)_2$ 要简单些，但由于在计算卷积的过程中，所需的 N 次一般乘法是在全过程的中间阶段进行的，其时参与运算的数均为新码，故运算规则 $(6)_2$ 是不可少的.

美国麻省理工学院林肯研究室已在 1976 年利用此码作出了一个 FNT 的硬件，其字长为 16 位，$\alpha = \sqrt{2}$，$N = 64$.

2.3. 减 1 码 前一小节中讨论之新码，实质上是利用了在任意模 M 的剩余类环 Z_M 中，一次方程

$$A\hat{x} + B \equiv x \pmod{M}, \tag{1)_1}$$

当 A 与 M 互素(B 可任取)时，对任意给定的整数 $x \in Z_M$ 均存在唯一的解 $\hat{x} \in Z_M$，这一重要性质，从而建立了 Z_M 自身的一个一一对应关系 $x \longleftrightarrow \hat{x}$，故可取 $\hat{x}$ 之二进制码作为 x 的新码. 因此，对任意与 M 互素的 A 和任意的 B，均可导出一种新的码来. 但是，为克服模 $2^b + 1$ 的运算中处理 $2^b = 1\ \overbrace{0 \cdots 0}^{b\text{个}}$ 时所遇到的困难，我们希望将 $1\ \overbrace{0 \cdots 0}^{b\text{个}}$ 作为数 0 的新码，即要求 $x = 0$ 时，$\hat{x} = \hat{0} = 2^b$. 易知，此条件当且仅当 $A \equiv B \pmod{2^b + 1}$ 时始能成立，故 $(1)_1$ 应取为

$$A(\hat{x} + 1) \equiv x \pmod{2^b + 1}, \tag{1)_2}$$

式中之 A 与 M 互素. 前面讨论的新码正是取 $A = 2$ 时所得的码.

如果在 $(1)_2$ 中取 $A = 1$，则有

$$\hat{x} + 1 \equiv x \pmod{2^b + 1}. \tag{1)_3}$$

故除 $x=0$ 之新码为 $1\overbrace{0\cdots0}^{b个}$ 外，$x\in Z_M$ 之新码就是 $x-\dot{1}$ 的二进制码，故称此新码为“减 1 码”。

显然，对减 1 码来说，其新、旧码之间的转换关系比较简单。但由于对新、旧码间的对应关系 (1)₂ 并无实质性的改进，故可预见，与前面的新码相比，减 1 码之间的模 2^b+1 运算是不可能有实质上的改进和简化的。事实上，可完全仿照上节的推理证明，减 1码间模 2^b+1 的运算规则，除一般乘法外，其加法、取负和乘 2^k 的乘法均与前述新码的运算规则完全相同。而其一般乘法为

$$\hat{A}\widehat{\otimes}\hat{B}=\{\widehat{\oplus}_{k=0}^{b-1}[(\widehat{a_k 2^k})\widehat{\otimes}\hat{B}]\}\widehat{\oplus}\hat{B},$$

这里，$\hat{A}=\sum_{k=0}^{b-1}a_k 2^k \neq 2^b$。 与 § 2.2. (6)₂ 相比，稍有简化。

§ 3. 字长与序列长度间的关系

在 FNT 的快速实现过程中，除在计算机上实现模 2^b+1 运算这样一个基本问题外，还有一个序列长度和字长的关系问题。这是因为在 FNT 中，字长 b、序列长度 N 和所选用的 α 三者之间有着严格的相互制约关系，从而不能随意地选取。

由于在 FNT 的快速计算中，所用乘法都是乘 α 的方幂，故取 α 为 $\sqrt{2}=2^{\frac{3b}{4}}-2^{\frac{b}{4}}$ 的偶次幂(即 2 的方幂)最为简单。稍次是取 α 为 $\sqrt{2}$ 的奇次幂，此时只是在第一次叠代中才需乘 $\sqrt{2}$ 的奇次幂(即乘 2 的幂后再乘一次 $\sqrt{2}$)，而在其余各次叠代中却仍是乘 $\sqrt{2}$ 的偶次幂。因此，在快速实现 FNT 时，我们总是取 α 为 $\sqrt{2}$ 的方幂。

通常情形下，序列长度 N 是事先给定的。我们的问题就是，在序列长度 $N=2^m$ 给定和 α 取 $\sqrt{2}$ 的方幂的情况下，怎样来选择 $\sqrt{2}$ 的幂指数和字长 $b=2^t$。

1. 一维的情形是简单的。由第三章 § 4 知，若令 t_0 是适合为

$$2^{2^t-1} \geqslant \min\left\{|x_n|_{\max}\cdot\sum_{k=0}^{N-1}|h_k|,\ |h_n|_{\max}\cdot\sum_{k=0}^{N-1}|x_k|\right\}$$

之最小正整数，则只需选取

$$t \geqslant \max\{t_0,\ m-2\},\ \alpha = (\sqrt{2})^{2^{t+2-m}}$$

即可。因此 M 的最小可取值为 $2^{2^{m-2}}+1$，亦即所需字长最少为 $2^{m-2}=\frac{1}{4}N$。

由于通常的计算机之字长在 64 位以下，故用 α 取 $\sqrt{2}$ 之方幂的一维 FNT 可卷积的序列长度最长可达 $64\times4=256=2^8$。

2. 当 $N=2^m\geqslant2^9$ 时，在普通计算机上就不能用 α 取 $\sqrt{2}$ 之方幂的一维 FNT 计算序列的卷积。此时可考虑采用二维 FNT 来进行计算。由第三章 §7 知

1）当 $N=2^m$，$2\nmid m$ 时，可取 $N_1=2^{\frac{m-1}{2}}$，$N_2=2^{\frac{m+1}{2}}$，$t\geqslant\max\left\{t_0,\ \frac{m-3}{2}\right\}$，$\alpha_1=\alpha_2=(\sqrt{2})^{2^{t-\frac{m-3}{2}}}$。

由此可知，当 $t_0\geqslant m-2$ 时，用 α 取 $\sqrt{2}$ 之方幂的一维 FNT 与用二维 FNT 所需字长均至少为 2^{t_0}，故此时用二维 FNT 亦不能缩短字长。当 $t_0<m-2$ 时，用二维 FNT 所需之字长最短可取为 2^{t_0} 或 $2^{\frac{m-3}{2}}$，均小于 2^{m-2}，故可使字长缩短。但最短不能短于 $2^{\frac{m-3}{2}}=\sqrt{N/8}$。从而在字长为 32 或 64 位的计算机上，用 α 取 $\sqrt{2}$ 之方幂的二维 FNT 可卷积 m 为奇的最大序列长度为 2^{13} 或 2^{15}。

2）当 $N=2^m$，$2|m$ 时，可取 $N_1=2^{\frac{m}{2}-1}$，$N_2=2^{\frac{m}{2}+1}$（或 $N_1=N_2=2^{\frac{m}{2}}$），

$$t\geqslant\max\left\{t_0,\ \frac{m}{2}-1\right\},\ \alpha_1（或\ \alpha_2）=(\sqrt{2})^{2^{t+2-\frac{m}{2}}},$$

$$\alpha_2（或\ \alpha_1）=(\sqrt{2})^{2^{t+1-\frac{m}{2}}}.$$

易知当 $t_0 < m-2$ 时，可用 α 取 $\sqrt{2}$ 之方幂的二维 FNT 缩短一维 FNT 所需的字长，但最短不能短于 $2^{\frac{m-2}{2}} = \sqrt{N/4}$. 从而在字长为 32 或 64 位的计算机上，用 α 取 $\sqrt{2}$ 之方幂的二维 FNT 可卷积 m 为偶之最大序列长度可达 2^{12} 或 2^{14}. 如在上节中提到的美国麻省理工学院所作 16 位 FNT 硬件上，用 $\alpha_1 = 2$，$\alpha_2 = \sqrt{2}$ 或 $\alpha_1 = \alpha_2 = \sqrt{2}$ 的二维 FNT 就可分别计算长为 2^{10} 或 2^{11} 的卷积.

3. 在一些特殊需要中，有可能 $N = 2^m > 2^{15}$. 此时可考虑采用三维 FNT 来进行计算. 由第三章 § 8 知

1) 当 $N = 2^m$, $m \equiv 0 \pmod 3$ 时，可取 $N_1 = 2^{\frac{m}{3}-1}$, $N_2 = 2^{\frac{m}{3}}$, $N_3 = 2^{\frac{m}{3}+1}$（或 $N_1 = N_2 = N_3 = 2^{\frac{m}{3}}$），

$$t \geqslant \max\left\{t_0, \frac{m}{3}-1\right\},\ \alpha_1\text{（或 }\alpha_3\text{）} = (\sqrt{2})^{2^{t+2-\frac{m}{3}}},$$

$$\alpha_2 = \alpha_3\text{（或 }\alpha_1\text{）} = (\sqrt{2})^{2^{t+1-\frac{m}{3}}}.$$

故此时所需之最短字长为 $2^{\frac{m}{3}-1} = \sqrt[3]{N/8}$. 从而在字长为 32 或 64 位的计算机上，用 α 取 $\sqrt{2}$ 之幂的三维 FNT 可卷积 m 为 3 之倍数的最大序列长度可达 2^{18} 或 2^{21}.

2) 当 $N = 2^m$, $m \equiv 1 \pmod 3$ 时，可取 $N_1 = N_2 = 2^{\frac{m-1}{3}}$, $N_3 = 2^{\frac{m+2}{3}}$,

$$t \geqslant \max\left\{t_0, \frac{m-4}{3}\right\},\ \alpha_1 = \alpha_2 = \alpha_3 = (\sqrt{2})^{2^{t-\frac{m-4}{3}}}.$$

故此时所需之最短字长为 $2^{\frac{m-4}{3}} = \sqrt[3]{N/16}$. 从而在字长为 32 或 64 位的计算机上，用 α 取 $\sqrt{2}$ 之方幂的三维 FNT 可卷积 m 模 3 余 1 的最大序列长度可达 2^{19} 或 2^{22}.

3) 当 $N = 2^m$, $m \equiv 2 \pmod 3$ 时，可取 $N_1 = N_2 = 2^{\frac{m-2}{3}}$, $N_3 = 2^{\frac{m+4}{3}}$（或 $N_1 = 2^{\frac{m-2}{3}}$, $N_2 = N_3 = 2^{\frac{m+1}{3}}$），

表 2.　$N=2^m$ 时，最短字长和 N_i，α_i 的选择

m (mod 6)		$m\equiv 0$	$m\equiv 2$	$m\equiv 4$	$m\equiv 1$	$m\equiv 3$	$m\equiv 5$
三维FNT	最短字长 b	$\sqrt[3]{\frac{N}{8}}$	$\sqrt[3]{\frac{N}{4}}$	$\sqrt[3]{\frac{N}{16}}$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
	N_1，N_2，N_3 的选择	$2N_1=N_2=\frac{1}{2}N_3=\sqrt[3]{N}$ (或 $N_1=N_2=N_3=\sqrt[3]{N}$)	$2N_1=2N_2=\frac{1}{2}N_3=\sqrt[3]{2N}$ (或 $2N_1=N_2=N_3=\sqrt[3]{2N}$)	$N_1=N_2=\frac{1}{2}N_3=\sqrt[3]{\frac{N}{2}}$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
	α_1，α_2，α_3 的选择	$\alpha_1=2$，$\alpha_2=\alpha_3=\sqrt{2}$ (或 $\alpha_1=\alpha_2=\sqrt{2}$，$\alpha_3=2$)	$\alpha_1=\alpha_2=2$，$\alpha_3=\sqrt{2}$ (或 $\alpha_1=\alpha_3=2$，$\alpha_2=\sqrt{2}$)	$\alpha_1=\alpha_2=\alpha_3=\sqrt{2}$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
二维FNT	最短字长 b	$\sqrt{\frac{N}{4}}$			$\sqrt{\frac{N}{8}}$		
	N_1，N_2 的选择	$N_1=\sqrt{\frac{N}{4}}$，$N_2=\sqrt{4N}$ (或 $N_1=N_2=\sqrt{N}$)			$N_1=\sqrt{\frac{N}{2}}$，$N_2=\sqrt{2N}$		
	α_1，α_2 的选择	$\alpha_1=2$，$\alpha_2=\sqrt{2}$ (或 $\alpha_1=\sqrt{2}$，$\alpha_1=2$)			$\alpha_1=\alpha_2=\sqrt{2}$		
一维FNT	最短字长 b	$\frac{N}{4}$					
	N	N					
	α	$\alpha=\sqrt{2}$					

表 3. 一、二、三维 FNT 计算一维循环卷积所需乘、加法次数

$m\ (\mathrm{mod}\ 6)$			$m\equiv 0$	$m\equiv 2$	$m\equiv 4$	$m\equiv 1$	$m\equiv 3$	$m\equiv 5$
三维 FNT	N_1, N_2, N_3		$2N_1=N_2=\frac{1}{2}N_3=\sqrt[3]{N}$	$2N_1=2N_2=\frac{1}{2}N_3=\sqrt[3]{2N}$	$N_1=N_2=\frac{1}{2}N_3=\sqrt[3]{\frac{N}{2}}$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
	计算量	乘	$\frac{13}{3}N\log_2 N-14N+19N^{2/3}$	$\frac{13}{3}N\log_2 N-\frac{41}{3}N+\frac{33}{\sqrt[3]{2}}N^{2/3}$	$\frac{13}{3}N\log_2 N-\frac{37}{3}N+13\sqrt[3]{2}N^{2/3}$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
		加	$\frac{26}{3}N\log_2 N+8N$	$\frac{26}{3}N\log_2 N+\frac{26}{3}N$	$\frac{26}{3}N\log_2 N+\frac{34}{3}N$	同 $m\equiv 4$	同 $m\equiv 0$	同 $m\equiv 2$
二维 FNT	N_1, N_2		$N_1=\sqrt{\frac{N}{4}},\quad N_2=\sqrt{4N}$			$N_1=\sqrt{\frac{N}{2}},\quad N_2=\sqrt{2N}$		
	计算量	乘	$\frac{5}{2}N\log_2 N-5N+8N^{1/2}$			$\frac{5}{2}N\log_2 N-\frac{9}{2}N+5\sqrt{2}N^{1/2}$		
		加	$5N\log_2 N+4N$			$5N\log_2 N+5N$		
一维 FNT	N		$N=2^m$					
	计算量	乘	$\frac{3}{2}N\log_2 N-2N+3$					
		加	$3N\log_2 N$					

$$t \geqslant \max\left\{t_0, \frac{m-2}{3}\right\}, \quad \alpha_1 = \alpha_2\,(\text{或 } \alpha_3) = (\sqrt{2})^{2^{t+1-\frac{m-2}{3}}},$$

$$\alpha_3\,(\text{或 } \alpha_2) = (\sqrt{2})^{2^{t-\frac{m-2}{3}}}.$$

故此时所需之最短字长为 $2^{\frac{m-2}{3}} = \sqrt[3]{N/4}$. 从而在字长为 32 或 64 位的计算机上，用 α 取 $\sqrt{2}$ 之方幂的三维 FNT 可卷积 m 模 3 余 2 的最大序列长度可达 2^{17} 或 2^{20}.

值得注意的是，用 α 取 $\sqrt{2}$ 之方幂的二维 FNT 计算一维卷积时，序列长度 $N = 2^{2k+2}$ 和 2^{2k+3} 所需之字长同为 2^k. 而用 α 取 $\sqrt{2}$ 之幂的三维 FNT 计算一维卷积时，序列长度 $N = 2^{3k+2}$, 2^{3k+3} 和 2^{3k+4} 所需之字长亦同为 2^k.

综上所述，列表如上面表 2.

最后还要指出，用二、三维 FNT 计算一维卷积虽常可缩短用一维 FNT 计算时所需的字长，但其计算量却有相当的增加. 究竟增加多少呢? 对此我们曾作过较详细的讨论，由于讨论过程冗长而不困难，故在此将其略去，而只将所得结果列在上面表 3 里.

§4. 用快速 Fermat 数变换与 FFT 计算卷积运算量的比较

本节中，我们将尽可能详尽地比较用快速 FNT 和用 FFT 计算卷积时分别所需运算量的多少. 由 §1. 知，快速 FNT 与 FFT 有相同的流向图，所不同者为，在快速 FNT 中可取 $\alpha=2$，而在 FFT 中 $\alpha = e^{\frac{2\pi i}{N}}$; 快速 FNT 中的运算是模 2^b+1 的运算，而在 FFT 中的运算是普通复数的运算. 因此，只从它们各自所需之乘、加(减)法次数是看不出什么优劣的. 故需寻求一个统一的衡量标准.

显然，一个复数加(减)法相当于 2 个实数加(减)法；一个复数乘法相当于 4 个实数乘法和 2 个实数加法. 而一个 b 位实数的乘

法可平均地看作$\frac{b}{2}$个乘2的方幂的乘法和$\frac{b}{2}$个b位实数的加法．从而一个实、虚部均为b位的复数乘法就相当于$2b$个移位（即乘2的方幂）和$2(b+1)$个b位实数的加法．

由§2.2.知，一个模2^b+1的加法最多相当于2个b位实数的加法；视“取补”为一个减法，则一个模2^b+1的减法(取负相加)最多相当于3个b位实数的加(减)法；一个模2^b+1的乘2^k的乘法相当于1个移位和一次b位实数的减法；一个模2^b+1的一般乘法平均相当于$\frac{b}{2}$个模2^b+1的乘2^k的乘法和$\frac{b}{2}$个模2^b+1的加法，从而相当于$\frac{b}{2}$个移位和$\frac{3}{2}b$个b位实数的加(减)法．

由此，我们可将计算机上的普通加法和移位(自然每次不必是移一位)这两种基本运算作为统一的衡量标准来进行比较．

设$N=2^m$，$\alpha=2$，$b=\frac{N}{2}=2^{m-1}$．由§1.知，作一个FFT或FNT各共需复数的或模2^b+1的加、减法各$\frac{1}{2}mN$次，乘法

$$\frac{1}{2}(m-2)N+1\approx\frac{1}{2}(m-2)N \text{ 次}.$$

因此，作一个FFT共需

移位

$$\frac{1}{2}(m-2)N\cdot 2b=\frac{1}{2}(m-2)N^2 \text{ 次}, \tag{1}$$

加(减)法

$$\frac{1}{2}mN\cdot 2+\frac{1}{2}mN\cdot 2+\frac{1}{2}(m-2)N\cdot 2(b+1)$$

$$=\frac{1}{2}(m-2)N^2+3mN-2N \text{ 次}. \tag{2}$$

而作一个FNT共需

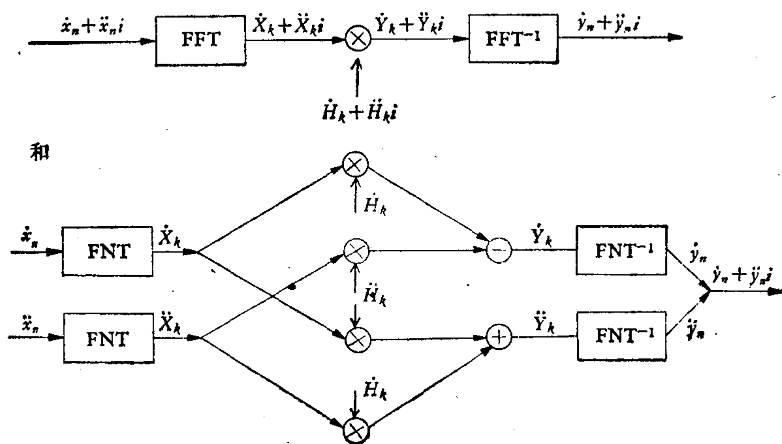
移位

$$\frac{1}{2}(m-2)N \text{ 次}, \tag{3}$$

加(减)法

$$\frac{1}{2}mN\cdot 2+\frac{1}{2}mN\cdot 3+\frac{1}{2}(m-2)N$$
$$=3mN-N \text{ 次}. \tag{4}$$

下面进一步考虑整个卷积的计算过程. 一则，在实际应用中序列h_n都是已知的，其 FNT 或 DFT 均可事先算出，故可不考虑其计算量. 二则，在实际应用中信号x_n常取复数形式，用 FFT 可直接进行处理，而用快速 FNT 则必须分别对其实部和虚部进行处理. 如用$\dot{a}$和$\ddot{a}$分别表复数a的实部和虚部，即$\dot{a}+\ddot{a}i=a$，则可简单地把用 FFT 和用快速 FNT 计算卷积的过程表示为如下的框图：



由此可知，在用 FFT 计算复信号卷积的过程中，共需一个FFT和一个 FFT^{-1}(表示FFT之逆)以及N次复数乘法. 再注意 FFT^{-1}较 FFT 需多进行N次乘N^{-1}(它是 2 的方幂)的乘法，由 (1), (2) 便知，此时共需

移位

$$2\cdot\frac{1}{2}(m-2)N^2+N\cdot 2b+N=(m-1)N^2+N \text{ 次},$$

加(减)法

$$2\cdot\left\{\frac{1}{2}(m-2)N^2+3mN-2N\right\}+N\cdot 2(b+1)$$

$$=(m-1)N^2+6mN-2N \text{ 次}.$$

而在用快速 FNT 计算复信号卷积的过程中，共需 2 个 FNT、2 个 FNT^{-1} 和$4N$次模 2^b+1 的一般乘法以及N次模 2^b+1 的加法、N次模 2^b+1 的减法. 再注意 FNT^{-1} 中多出的N次模 2^b+1 乘 N^{-1}(它是 2 的方幂)的乘法，由 (3)、(4) 便知，此时共需

移位

$$4\cdot\frac{1}{2}(m-2)N+4N\cdot\frac{b}{2}+2N$$

$$=N^2+2mN-2N \text{ 次},$$

加(减)法

$$4\cdot(3mN-N)+4N\cdot\frac{3}{2}b+2N+3N+2N$$

$$=3N^2+12mN+3N \text{ 次}.$$

把两种运算总起来看，用快速 FNT 和用 FFT 计算复数卷积时，其计算量的比大约是 2: $m-1$，故当m稍大时，前者较后者所需的计算量将有成倍的节约. 但应指出的是，这里对硬件的实现和节约并未予以考虑.

第五章　代数数论初步

为了计算代数整数的卷积，需要推广数论变换的概念，在一般的代数数域里的整数剩余类环上构造 DFT. 为此本章介绍一些代数数论的基础知识. 为突出重点，其中部分定理略去了证明，如读者需要时，可查阅有关参考书籍.

§1. 环　和　域

这里先扼要的介绍一般的环、域的概念和有关有限域的一些结果.

所谓具有一个加法和一个乘法运算的系统是指元素 $a, b, \cdots$ 的一个集合. 在其中定义了两个运算法则，使集合的任意两个元素都唯一地确定一个和 $a+b$ 以及一个积 $a\cdot b$，它们仍属于这个集合.

1）一个具有两个运算的系统称为环，如果对于系统中所有元素，以下的运算规律成立：

加法结合律　$(a+b)+c=a+(b+c)$，

加法交换律　$a+b=b+a$，

有零元素 0，它具有性质 $a+0=a$，

每个元素 a 均有负元素 $-a$，它具有性质 $a+(-a)=0$，

乘法结合律　$a(bc)=(ab)c$，

左分配律　$a(b+c)=ab+ac$，

右分配律　$(b+c)a=ba+ca$.

2）设 F 是一个至少含两个元素的环，且其乘法还适合：

乘法交换律　$ab=ba$，

有单位元素 e，它具有性质 $ea=a$，

任一非零元素 a 都有逆元素 a^{-1} 存在，满足 $a^{-1}a = e$.
此时称 F 为一个域.

3）两个环或域 F 与 F' 称为同构的，如果存在一个 F 到 F' 上的一一映射 σ，适合条件

$$\sigma(a+b)=\sigma(a)+\sigma(b),$$
$$\sigma(ab)=\sigma(a)\sigma(b).$$

4）域 F 中一个非空子集 F_1 对 F 的运算也组成一个域，则称 F_1 为 F 的一个子域，称 F 为 F_1 的扩域，记为 $F_1\subseteq F$.

5）设 F 是一个域，以 $F[x]$ 记域 F 上的全体多项式的集合，易知 $F[x]$ 对于多项式的加法和乘法构成一个可换环.

如以 F' 表示 F 的任一扩域，那么 $F[x]$ 中的多项式 $g(x)|f(x)$ 或 $g(x)\nmid f(x)$ 的性质在 $F'[x]$ 中仍保持不变.

6）域 F 中的元素个数有限时称有限域. 如 Z_p 就是含 p 个元素的有限域. 有时也用 $GF(p)$ 来记 Z_p.

有限域元素的个数一定是素数的方幂. 反之，对任给的素数 p 和正整数 n，均存在元素个数为 p^n 的有限域. 且可证明元素个数相同的任意两个有限域都是同构的，故常记元素个数为 p^n 的有限域为 $GF(p^n)$.

$GF(p^n)$ 中全部适合 $x^{p^m}-x=0$，$(m|n)$ 的元素构成唯一的一个元素个数为 p^m 的子域 $GF(p^m)$. 反之，若 $GF(p^m)$ 是 $GF(p^n)$ 的子域，则有 $m|n$.

7）设 $F=GF(p^n)$，F 中存在 d 次本原单位根的充分必要条件为 $d|p^n-1$. 且当 $d|p^n-1$ 时，F 中有 $\varphi(d)$ 个 d 次本原单位根（本原单位根与 Z_M 上的定义相类似）.

§2. 代数数和代数数域

定义. 如果一个复数 θ 是系数为有理数的一代数方程

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0 \qquad (1)$$

之根，则复数 θ 称为代数数.

例如，$i=\sqrt{-1}$，$\sqrt{2}$，$\sqrt[5]{3}$ 等等都是代数数。

如果(1)不可约，即指 $f(x)$ 不能分解成两个次数小于 n 的有理系数多项式的乘积，且 $a_n \neq 0$，则称 $n = \partial^0 f(x)$ 为 θ 的次数。

如果 (1) 式为不可约，并以

$$\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)} \tag{2}$$

表示 $f(x)=0$ 的全部根，则有 $\theta^{(j)} \neq \theta^{(k)}$，$(j \neq k)$.

定义. 若 θ 为一首项系数为 1，其它系数为有理整数的不可约多项式的根，则 θ 称为代数整数，当 θ 及 θ^{-1} 都是代数整数时，θ 称为单位数.

例如 i 就是一个单位数.

设 θ 是一个 n 次代数数，R 表示有理数域，我们有下面的定理.

定理 1. 所有形如

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1},\quad a_i \in R\ (i=0,1,\cdots,n-1) \tag{3}$$

的数集对于普通的加法和乘法成域，而且 (3) 给出的数各不相同.

证. 如果

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1},$$

而且有某个 $a_k \neq b_k$，$0 \leqslant k \leqslant n-1$，则 θ 适合一个次数不高于 $n-1$ 次的多项式，与 θ 的次数是 n 矛盾，故(3)给出的数各不相同.

设 $f(x)$ 为一 θ 所适合的 n 次不可约多项式，又设

$$\alpha = a(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1},$$

$$\beta = b(\theta) = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1},$$

显然

$$\alpha \pm \beta = \sum_{i=0}^{n-1} (a_i \pm b_i)\theta^i$$

亦为(3)之形式的数，再由多项式的带余除法知存在有理系数多项式 $q(x)$ 和 $r(x)$ 满足

$$a(x)b(x) = q(x)f(x) + r(x),$$

$r(x)=0$ 或 $\partial^0 r(x) < \partial^0 f(x) = n$，故

$$\alpha\beta = a(\theta)b(\theta) = r(\theta)$$

仍为(3)之形状的数. 最后设 $\beta \neq 0$, 则 $(b(x), f(x)) = 1$,故存在有理系数多项式 $s(x)$及 $t(x)$,且 $\partial^0 s(x) < \partial^0 f(x)$, 使

$$s(x)b(x) + t(x)f(x) = 1$$

故有 $\beta^{-1} = s(\theta)$. 证完.

定义. 定理 1 中所得的域称为在有理数域 R 上添加 θ 所得的单扩张,以 $R(\theta)$ 表示. 称 θ 的次数为 $R(\theta)$ 的次数. 我们有

定理 2. 设 $R(\theta_1, \cdots, \theta_n)$ 表示由$\theta_1, \cdots, \theta_n$ 的所有有理函数组成的域, $\theta_1, \cdots, \theta_n$ 都是代数数,则有代数数 θ 存在,使 $R(\theta) = R(\theta_1, \cdots, \theta_n)$.

定理 3. 如果 D 过所有不等于 1 的无平方因子的整数, 则 $R(\sqrt{D})$ 经过所有的二次域.

证. 命$R(\theta)$为任一个二次域,而θ所适合的不可约多项式为 $ax^2 + bx + c$, 不失一般, a, b, c 可设为有理整数, 可设 $b^2 - 4ac = q^2D$, $D \neq 1$, 则因 $\theta = \dfrac{-b \pm q\sqrt{D}}{2a}$, 所以 $R(\theta) = R(\sqrt{D})$, 而 $R(\sqrt{D})$ 是二次域则是明显的. 证完.

设 $R(\theta)$ 为一 n 次代数数域,记 $\theta = \theta^{(1)}$, 并以 $\theta^{(2)}, \cdots, \theta^{(n)}$ 表示θ所适合的n 次不可约多项式的其它 $n-1$ 个根.

已知 $R(\theta)$ 中任一数 α 可表示成

$$\alpha = a(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1},$$
$$a_i \in R, \quad i = 0, 1, \cdots, n-1.$$

定义. 令 $\alpha^{(1)} = \alpha$, 称 $\alpha^{(k)} = a(\theta^{(k)})$, $(k = 2, \cdots, n)$ 为 α 的共轭数,又称

$$T(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n)},$$
$$N(\alpha) = \alpha^{(1)}\alpha^{(2)}\cdots\alpha^{(n)}$$

为 α 的迹与范数,我们有

$$T(\alpha + \beta) = T(\alpha) + T(\beta),$$
$$N(\alpha\beta) = N(\alpha)N(\beta).$$

且易知 $T(\alpha)$ 和 $N(\alpha)$ 均为 $\theta^{(1)}, \cdots, \theta^{(n)}$ 的对称多项式,故由对称多项式的性质,知道 $T(\alpha)$ 和 $N(\alpha)$ 均为有理数. 并且不难验证下

面的定理.

定理 4. 代数整数 α 为单位数的充分必要条件是

$$N(\alpha)=\pm 1.$$

设 F 是任一数域,则对于有理数域 R 的 n 次代数数 θ, 单扩张 $R(\theta)$, 以及共轭数 $\alpha^{(1)},\cdots,\alpha^{(n)}$ 等的定义可以完全类似地用来对于数域 F 定义, 把基域 R 换成 F 后, 以上相应的定理也都成立,这里就不再一一列出了.

下面我们就一般的数域 F 给出几个定理, 它自然对于有理数域 R 也是成立的.

设 θ 是 F 上的一个 n 次代数数,扩域 $F(\theta)$ 的每一个数 α 可表示成 $\alpha=a(\theta)$, $a(x)$ 是 $F[x]$ 中一个次数低于 n 的多项式.

定理 5. 设 $\theta=\theta^{(1)},\theta^{(2)},\cdots,\theta^{(n)}$ 为 θ 的共轭数, $\alpha=a(\theta)$ 是 F 上的一个 m 次代数数, 又设 α 所适合的 F 上的不可约多项式是 $h(x)$, $\partial^0 h(x)=m$, 如令

$$g(x)=\prod_{i=1}^{n}(x-\alpha^{(i)}),$$

则 $g(x)$ 为系数在 F 上的多项式,且 $m|n$,

$$g(x)=c(h(x))^{n/m},\quad c\in F.$$

证. 由对称多项式定理,立刻得 $g(x)\in F[x]$, 因为

$$h(\alpha)=h(a(\theta))=0,$$

所以

$$h(\alpha^{(i)})=h(a(\theta^{(i)}))=0\quad(i=1,2,\cdots,n),$$

即 $g(x)=0$ 的每一个根也是 $h(x)=0$ 的根,因 $h(x)$ 不可约,故 $h(x)|g(x)$. 设 $g(x)=h(x)g_1(x)$, 若 $g_1(x)$ 为 F 中的一常数,则定理已证, 否则因 $g_1(x)=0$ 的根皆为 $h(x)=0$ 的根, 又有 $h(x)|g_1(x)$, 设 $g_1(x)=h(x)g_2(x)$, 继续进行下去,有限步后可得

$$g(x)=c(h(x))^{n/m},\quad m|n,\quad c\in F.$$

证完.

由定理可知，如果α是m次代数数，则在$\alpha^{(1)},\cdots,\alpha^{(n)}$中出现$m$个不同的数，设为$\alpha^{(i_1)},\cdots,\alpha^{(i_m)}$，$1=i_1<i_2<\cdots<i_m\leqslant n$，且每个数各出现$\frac{n}{m}$次，而$\alpha^{(i_1)},\cdots,\alpha^{(i_m)}$恰好是$h(x)$的全部根.

定义. $h(x)$称为α在F上的定义多项式.

推论1. $F(\theta)$中的任一个数在F上的次数至多是n，次数比n小的数，不能生成$F(\theta)$.

推论2. 如果$\alpha_1,\cdots,\alpha_k$均是$F(\theta)$中的数，且

$$E(\alpha_1,\cdots,\alpha_k)=0,$$

则

$$E(\alpha_1^{(i)},\cdots,\alpha_k^{(i)})=0\quad(i=1,\cdots,n),$$

这里$E(x_1,\cdots,x_k)$是F上的多项式.

定义. 任一个域F'包含一个给定的域F，则叫F'是F的一个扩张，如果F'的每一个元在F上是代数的，则叫F'是F的代数扩张，否则叫超越扩张.

定义. F'的元$w_1,w_2,\cdots,w_n$在F上是线性无关的，如果由

$$a_1w_1+a_2w_2+\cdots+a_nw_n=0,\ a_i\in F\ (i=1,\cdots,n)$$

可以推出$a_1=a_2=\cdots=a_n=0$.

一个F的扩张F'称为F的有限扩张，如果存在有限个$w_1,\cdots,w_n$使得F'的每一个元α都能表示成

$$\alpha=a_1w_1+\cdots+a_nw_n,\ a_i\in F\quad(i=1,\cdots,n),$$

则称$w_1,\cdots,w_n$是F'在F上的一组生成系，如果同时$w_1,\cdots,w_n$在F上又是线性无关的，那么称$w_1,\cdots,w_n$是F'在F上的一组基底.

定理6. 每一个有限扩张$F'\supseteq F$有一组F'在F上的基底，如基底由n个元组成，则

(1) F'的任意$n+1$个元在F上不是无关的.

(2) 任一组基底均有n个元.

(3) 任意n个无关的元组成一组基底.

这是代数中熟知的定理，在下节里我们对F是有理数域的情

形给出证明.

定理7. 每一个有限扩张 $F'\supseteq F$ 在 F 上是代数的(即 F' 的每一元在 F 上是代数的).

这也是代数中熟知的结果.

定理6告诉我们,F' 在 F 上的基底中含 n 个元与基底的选择无关,故有下述定义.

定义. 设 $w_1,\cdots,w_n$ 是 F' 在 F 上的一组基底,称 n 是 F' 在 F 上的次数,记为 $(F'|F)=n$. (这与前面定义 $R(\theta)$ 的次数是一致的).

设 $\beta\in F(\theta)$, $\beta=\beta^{(1)}$, $\beta^{(2)}$, $\cdots$, $\beta^{(n)}$ 是 F 上的共轭数, 我们有:

定义. $F(\beta^{(i)})$ 和 $F(\beta^{(j)})$ 称为 F 上的共轭域,如果有 $F(\beta)=F(\beta^{(j)})$ $(j=1,2,\cdots,n)$, 则称 $F(\beta)$ 在 F 上是正规的.

定理8. 设 $F''\supseteq F'\supseteq F$, $(F''|F')=q$, $(F'|F)=m$, $(F''|F)=n$, $F''=F(\xi)$, $\xi^{(1)},\cdots,\xi^{(n)}$ 是 F 上的共轭数, $F'=F(\theta)$, $\theta^{(1)},\cdots,\theta^{(m)}$ 是 F 上的共轭数,则

(1) $qm=n$.

(2) 可以将 $\xi^{(1)},\cdots,\xi^{(n)}$ 分成 m 组数, 每组含 q 个数, 使得每组的 q 个数恰分别为域 $F(\theta^{(i)})$ 上的共轭数 $(i=1,\cdots,m)$.

证. (1) 是代数中熟知的结果, 这里略去不证. 现证 (2), 由于 $(F''|F')=q$, 故 ξ 满足系数在 F' 上的 q 次不可约多项式,设为 $f(x)$, 再设 $f^{(1)}(x)=f(x)$, $f^{(2)}(x)$, $\cdots$, $f^{(m)}(x)$, $f^{(i)}(x)$ 表示把 $f(x)$ 的每一个系数分别换成它们在 F 上的第 i 个共轭数, 而令

$$\varphi(x)=\prod_{i=1}^{m}f^{(i)}(x),$$

$\varphi(x)$的系数是 $\theta^{(1)},\cdots,\theta^{(m)}$ 的对称多项式(系数在 F 中),故 $\varphi(x)$ 的系数在 F 中, 而 $\varphi(\xi)=0$, $\partial^0\varphi(x)=n$, 因此 $\xi^{(1)},\cdots,\xi^{(n)}$ 恰为 $\varphi(x)$ 的全部根,又因共轭域是彼此同构的, 所以 $f^{(i)}(x)$ 在域 $F(\theta^{(i)})$ 上不可约. 证完.

定理9. 设 $F'=F(\theta)$, $w_1,\cdots,w_n$ 是 F' 在 F 上的一组基

底.

$$w_i w_j = \sum_{l=1}^{n} c_{ijl} w_l \quad (i, j = 1, \cdots, n), \quad c_{ijl} \in F,$$

α 是 F' 的任一 n 次元.

$$\alpha = c_1 w_1 + \cdots + c_n w_n, \quad c_i \in F (i = 1, 2, \cdots, n),$$

则有

$$\Phi(t, c_1, \cdots, c_n) = (-1)^n \prod_{i=1}^{n} (t - \alpha^{(i)}), \tag{4}$$

其中 $\Phi(t, c_1, \cdots, c_n)$ 为行列式

$$\left| \sum_{j=1}^{n} c_j c_{ijl} - \delta_{il} t \right|, \quad \delta_{il} = \begin{cases} 0, & i \neq l, \\ 1, & i = l. \end{cases}$$

证. 考虑变量 $x_1, \cdots, x_n$ 的线性型

$$t = x_1 w_1 + \cdots + x_n w_n,$$

故

$$tw_i = \sum_{j=1}^{n} x_j w_i w_j = \sum_{j=1}^{n} \sum_{l=1}^{n} x_j c_{ijl} w_l$$

$$= \sum_{l=1}^{n} w_l \sum_{j=1}^{n} x_j c_{ijl},$$

且

$$\sum_{l=1}^{n} w_l \left[\sum_{j=1}^{n} x_j c_{ijl} - \delta_{il} t \right] = 0 \quad (i = 1, \cdots, n),$$

故有行列式

$$\left| \sum_{j=1}^{n} x_j c_{ijl} - \delta_{il} t \right| = \Phi(t, x_1, \cdots, x_n) = 0. \tag{5}$$

由于 $x_1 w_1 + \cdots + x_n w_n$ 是一个根,它的所有共轭也是 (5) 的根,由于 α 是 n 次的,所有共轭数不相同,故令 $x_i = c_i$, $(i = 1, \cdots, n)$,便得到了 (4). 证完.

推论. 如 α 是 F' 的任一元,则 α 在 F 上的定义多项式

$$h(x) | \Phi(x, c_1, \cdots, c_n).$$

例. θ 是$x^3+x+1=0$ 的一个根，求 $R(\theta)$ 中的数 $\alpha=\theta+\theta^2$ 所适合的方程，我们有 $\theta^2=-\theta-1$，故

$$\alpha=\theta+\theta^2$$
$$\alpha\theta=-1-\theta+\theta^2$$
$$\alpha\theta^2=-1-2\theta-\theta^2,$$

$$-\begin{vmatrix}-\alpha & 1 & 1\\ -1 & -1-\alpha & 1\\ -1 & -2 & -1-\alpha\end{vmatrix}=\alpha^3+2\alpha^2+5\alpha+1=0.$$

从定理 9 还可以推出下面的结果:

设 $\alpha=\sum\limits_{i=1}^{n} c_i w_i$ 是 F' 中的 n 次代数数，

$$d_{il}=\sum_{j=1}^{n} c_{ijl}c_j,$$

则

$$N(\alpha)=\alpha^{(1)}\cdots\alpha^{(n)}=|d_{il}|,$$

$$T(\alpha)=\alpha^{(1)}+\cdots+\alpha^{(n)}=\sum_{j=1}^{n} d_{jj}.$$

因此，在上例中，因 x^3+2x^2+5x+1 是不可约的，α 是三次代数数，故

$$N(\theta^2+\theta)=-1,\qquad T(\theta^2+\theta)=-2.$$

从下节开始，如无特别声明，均考虑有理数域 R 的代数扩张。

§3. $R(\theta)$ 的基底和整底

仍考虑 n 次域$R(\theta)$，即 θ 是一个 n 次代数数，$1,\theta,\cdots,\theta^{n-1}$为 $R(\theta)$ 的一组基底，我们有

定理 1. $R(\theta)$ 的任一基底中所含数的个数都等于 n.

证. 设 $\alpha_1,\cdots,\alpha_m$ 和 $\beta_1,\cdots,\beta_{m'}$ 为 $R(\theta)$ 的任意两组基，只需证明 $m=m'$，否则，可设 $m>m'$，故有有理数 a_{ij} 及 b_{ij} 使

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}=\begin{pmatrix}a_{11}\cdots a_{1m'}0\cdots 0\\ a_{21}\cdots a_{2m'}0\cdots 0\\ \cdots\cdots\cdots\cdots\\ a_{m1}\cdots a_{mm'}0\cdots 0\end{pmatrix}\begin{pmatrix}\beta_1\\ \vdots\\ \beta_{m'}\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

和

$$\begin{pmatrix}\beta_1\\ \vdots\\ \beta_{m'}\\ 0\\ \vdots\\ 0\end{pmatrix}=\begin{pmatrix}b_{11}\cdots b_{1m}\\ b_{21}\cdots b_{2m}\\ \cdots\cdots\cdots\\ b_{m'1}\cdots b_{m'm}\\ 0\cdots 0\\ \cdots\cdots\cdots\\ 0\cdots 0\end{pmatrix}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}.$$

此处 (a_{ij}) 和 (b_{ij}) 都是 $m\times m$ 阶方阵，于是得

$$\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix}=(a_{ij})(b_{ij})\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_m\end{pmatrix},$$

因 $\alpha_1,\cdots,\alpha_m$ 是线性无关的，故必须有 $(a_{ij})(b_{ij})=I$，而行列式 $|a_{ij}|=|b_{ij}|=0$，这是矛盾结果．证完．

若 $\alpha_1,\cdots,\alpha_n$ 及 $\beta_1,\cdots,\beta_n$ 为 $R(\theta)$ 的两组基底，则由定义，易知有有理数 $a_{jk}(1\leqslant j,k\leqslant n)$ 使

$$\alpha_j=\sum_{k=1}^{n}a_{jk}\beta_k \qquad (1\leqslant j\leqslant n),$$

且行列式

$$|a_{jk}|=\begin{vmatrix}a_{11}\cdots a_{1n}\\ \cdots\cdots\cdots\\ a_{n1}\cdots a_{nn}\end{vmatrix}\neq 0.$$

定义．设 $\alpha_1,\cdots,\alpha_n$ 是 $R(\theta)$ 中任意 n 个数，称

$$\triangle(\alpha_1,\cdots,\alpha_n)=\begin{vmatrix}\alpha_1^{(1)}\cdots\alpha_n^{(1)}\\ \cdots\cdots\cdots\\ \alpha_1^{(n)}\cdots\alpha_n^{(n)}\end{vmatrix}^2$$

为 $\alpha_1, \cdots, \alpha_n$ 的判别式.

定理 2. 判别式有下列性质:

1) $\triangle(\alpha_1, \cdots, \alpha_n)$ 为有理数,特别地,如果 $\alpha_1, \cdots, \alpha_n$ 为代数整数,则 $\triangle(\alpha_1, \cdots, \alpha_n)$ 为有理整数.

2) 如果 $\alpha_1, \cdots, \alpha_n$ 和 $\beta_1, \cdots, \beta_n$ 为 $R(\theta)$ 的两组数,适合

$$\alpha_j = \sum_{k=1}^{n} a_{jk}\beta_k \qquad (1 \leqslant j \leqslant n),$$

则

$$\triangle(\alpha_1, \cdots, \alpha_n) = |a_{jk}|^2 \triangle(\beta_1, \cdots, \beta_n).$$

3) $\alpha_1, \cdots, \alpha_n$ 为 $R(\theta)$ 的一组基底的充分必要条件是

$$\triangle(\alpha_1, \cdots, \alpha_n) \neq 0.$$

证. 1) 因为 $\triangle(\alpha_1, \cdots, \alpha_n)$ 可表示成 $\theta^{(1)}, \cdots, \theta^{(n)}$ 的对称多项式,故结果可由对称多项式定理推出.

2) 设

$$\alpha_j = \sum_{k=1}^{n} h_{jk}\theta^{k-1}, \qquad \beta_j = \sum_{k=1}^{n} b_{jk}\theta^{k-1} \qquad (1 \leqslant j \leqslant n),$$

则由 $(h_{jk}) = (a_{jk})(b_{jk})$ 知

$$\alpha_j^{(l)} = \sum_{k=1}^{n} a_{jk}\beta_k^{(l)} \qquad (1 \leqslant j, l \leqslant n),$$

故

$$\triangle(\alpha_1, \cdots, \alpha_n) = |a_{jk}|^2 \begin{vmatrix} \beta_1^{(1)} & \cdots & \beta_n^{(1)} \\ \cdots & \cdots & \cdots \\ \beta_1^{(n)} & \cdots & \beta_n^{(n)} \end{vmatrix}^2 = |a_{jk}|^2 \triangle(\beta_1, \cdots, \beta_n).$$

3) 因为:

$$\triangle(1, \theta, \cdots, \theta^{n-1}) = \prod_{1 \leqslant j < k \leqslant n} (\theta^{(j)} - \theta^{(k)})^2 \neq 0,$$

由2) 可知对 $R(\theta)$ 的任一组基底 $\alpha_1, \cdots, \alpha_n$ 有 $\triangle(\alpha_1, \cdots, \alpha_n) \neq 0$,

反之,若 $\triangle(\alpha_1, \cdots, \alpha_n) \neq 0$, 设

$$\alpha_j = \sum_{k=1}^{n} b_{jk}\theta^{k-1} \qquad (1 \leqslant j \leqslant n),$$

则

$$\triangle(\alpha_1, \cdots, \alpha_n) = |b_{jk}|^2\triangle(1, \theta, \cdots, \theta^{n-1}).$$

所以 $|b_{jk}| \neq 0$，故能以 $\alpha_1, \cdots, \alpha_n$ 表示出 $1, \theta, \cdots, \theta^{n-1}$，即知 $R(\theta)$ 中任一数可经 $\alpha_1, \cdots, \alpha_n$ 唯一表示出，故 $\alpha_1, \cdots, \alpha_n$ 是 $R(\theta)$ 的一组基底．证完．

定义．设 $w_1, \cdots, w_m$ 为 $R(\theta)$ 中的 m 个整数，若 $R(\theta)$ 中任一整数都能唯一地表示为如下形状

$$a_1w_1 + \cdots + a_mw_m,$$

其中 $a_1, \cdots, a_m$ 是有理整数，则称 $w_1, \cdots, w_n$ 为 $R(\theta)$ 中的一组整底．下面的定理说明了 $R(\theta)$ 中整底的存在．

定理 3．$R(\theta)$ 中的基底

$$w_1, \cdots, w_n,$$

其中诸 $w_j(1 \leqslant j \leqslant n)$ 皆为整数，且使 $|\triangle(w_1, \cdots, w_n)|$ 之值最小者，为一组整底．

证．易知存在有理整数 $q \neq 0$ 使 $q\theta$ 为整数，则 $1, q\theta, \cdots, (q\theta)^{n-1}$ 全为整数，由 $\triangle(1, q\theta, \cdots, (q\theta)^{n-1}) \neq 0$，故知有全为整数的基底存在．

现在设在所有以整数组成的基底中使 $|\triangle(w_1, \cdots, w_n)|$ 之值最小者为 $w_1, \cdots, w_n$，今证其即为 $R(\theta)$ 的整底，否则，有整数 w 存在，使

$$w = a_1w_1 + \cdots + a_nw_n,$$

其中 a_j 不全为有理整数，不妨设 a_1 非有理整数，设 $a_1 = g + t$，g 为有理整数，而 $0 < t < 1$，则

$$w_1' = w - gw_1 = tw_1 + a_2w_2 + \cdots + a_nw_n$$

也为整数，且

$$\triangle(w_1', w_2, \cdots, w_n) = t^2\triangle(w_1, \cdots, w_n) \neq 0.$$

故 $w_1', w_2, \cdots, w_n$ 也是 $R(\theta)$ 的一组由整数构成的基底，但

$$|\triangle(w_1', w_2, \cdots, w_n)| < |\triangle(w_1, \cdots, w_n)|,$$

这与 $|\triangle(w_1, \cdots, w_n)|$ 取最小值矛盾．证完．

由此定理可知整底也是基底，故整底中所含元素的个数也为 n.

定理 4. 整底的判别式相等.

证. 设 $w_1, \cdots, w_n$ 及 $w'_1, \cdots, w'_n$ 均为整底，故有

$$w_j = \sum_{k=1}^{n} a_{jk} w'_k, \quad w'_j = \sum_{k=1}^{n} b_{jk} w_k \quad (1 \leqslant j \leqslant n),$$

其中 a_{jk} 及 b_{jk} 均为有理整数，由此可得 $|a_{jk}||b_{jk}| = 1$，即得 $|a_{jk}| = |b_{jk}| = \pm 1$，故由定理 2 的 2) 得证.

定义. $R(\theta)$ 的整底的判别式称为域 $R(\theta)$ 的基数，常以$\triangle$来表示.

设 $\eta_1, \cdots, \eta_n$ 是任意 n 个整数，它们在整底 $w_1, \cdots, w_n$ 上的表达式为

$$\eta_i = \sum_{k=1}^{n} c_{ik} w_k \quad (i = 1, \cdots, n),$$

c_{ik} 是有理整数，因此

$$\triangle(\eta_1, \cdots, \eta_n) = |c_{ik}|^2 \triangle,$$

有理整数 $|c_{ik}|^2$ 叫 $\eta_1, \cdots, \eta_n$ 的指标. 又当 η 是一个 n 次整数时，我们称 $1, \eta, \cdots, \eta^{n-1}$ 的指标为 η 的指标，记为 index η.

定理 5. 设 $\eta_1, \cdots, \eta_n$ 是 $R(\theta)$ 在 R 上的一组基底，且 $\eta_1, \cdots, \eta_n$ 都是整数，则 $R(\theta)$ 中任一个整数 α 可写成如下的形状:

$$\alpha = \sum_{i=1}^{n} \frac{x_i \eta_i}{\triangle(\eta_1, \cdots, \eta_n)},$$

这里 x_i $(i = 1, \cdots, n)$ 是有理整数.

证. 因为 $\eta_1, \cdots, \eta_n$ 是一组基底，我们有

$$\alpha = \sum_{i=1}^{n} y_i \eta_i, \quad y_i \in R \quad (i=1, \cdots, n),$$

且

$$\alpha^{(k)} = \sum_{i=1}^{n} y_i \eta_i^{(k)} \quad (k=1, \cdots, n),$$

故

$$y_i=\frac{\pm\begin{vmatrix}\eta_1^{(1)}\cdots\eta_{i-1}^{(1)}\alpha^{(1)}\eta_{i+1}^{(1)}\cdots\eta_n^{(1)}\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \eta_1^{(n)}\cdots\eta_{i-1}^{(n)}\alpha^{(n)}\eta_{i+1}^{(n)}\cdots\eta_n^{(n)}\end{vmatrix}}{\sqrt{\triangle(\eta_1,\cdots,\eta_n)}}. \tag{1}$$

由 (1) 式我们看到 $y_i^2\triangle(\eta_1,\cdots,\eta_n)$ 是一个整数,故必是有理整数,而设 $x_i=y_i\triangle(\eta_1,\cdots,\eta_n)$, 则由 $y_i^2\triangle(\eta_1,\cdots,\eta_n)$ 是有理整数知x_i也是有理整数. 证完.

§4. 整除性和素数

定义. 设α,β为二代数整数,若存在一代数整数γ使$\alpha=\beta\gamma$,则称β可整除α, 记为$\beta|\alpha$, 否则称β不能整除α, 记为$\beta\nmid\alpha$.

由整除性,会联想到代数整数的因子分解问题,以后我们仅讨论在某一代数数域$R(\theta)$内的代数整数(常简称整数)分解的问题. 但因在$R(\theta)$中的单位数ε可能有无穷多个,这样任一整数α可表示为$\alpha=\varepsilon\varepsilon^{-1}\alpha$, 故其分解法就有无穷多种,为了除去这种平凡的因子分解,我们引进:

定义. 若两个整数α, β仅相差一单位数因子,则称α与β为相结合的.

定义. 对于非单位数的整数α, 若有$R(\theta)$中的整数β, γ, 均非单位数,且使

$$\alpha=\beta\gamma,$$

则称α在$R(\theta)$中可分解, 否则称α为$R(\theta)$中的不可分数或素数.

定理. $R(\theta)$中任一非单位数的整数可分解为素数的乘积.

证. 若α是素数,自不需证明. 如果

$$\alpha=\beta\gamma,$$

而β,γ均非单位数,则得

$$|N(\alpha)|=|N(\beta)||N(\gamma)|.$$

由于 β, γ 均非单位数，故自然数 $|N(\beta)|$，$|N(\gamma)|$ 为 $|N(\alpha)|$ 的真因数，即

$$|N(\alpha)| > |N(\beta)| > 1, \quad |N(\alpha)| > |N(\gamma)| > 1.$$

故可以对 $|N(\alpha)|$ 用归纳法证明之．证完．

如果相结合的因数看成相同的，那么整数的分解是否唯一呢？下面的例子告诉我们，即使在二次域里，唯一分解定理也不普遍成立．

例．在 $R(\sqrt{-5})$ 中唯一分解定理不成立．由于有

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

这里 $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ 显然都是整数，以后将看到它们都是 $R(\sqrt{-5})$ 中的素数．且因 $|N(2)| = 4$，$|N(3)| = 9$，$|N(1\pm\sqrt{-5})| = 6$，故 2，3 不与 $1+\sqrt{-5}$ 或 $1-\sqrt{-5}$ 相结合，可知在 $R(\sqrt{-5})$ 中唯一分解定理不成立．

§5. 理想数，同余

定义． 设 $R(\theta)$ 为一 n 次代数数域，$\alpha_1, \cdots, \alpha_q$ 为 $R(\theta)$ 内任意给定的 q 个整数，称所有形为

$$\eta_1\alpha_1 + \cdots + \eta_q\alpha_q, \quad (\eta_1, \cdots, \eta_q \text{为 } R(\theta) \text{ 中的整数}) \tag{1}$$

的整数所成的集合为由 $\alpha_1, \cdots, \alpha_q$ 生成的理想数，并以 $[\alpha_1, \cdots, \alpha_q]$ 记之，以后常用大写字母 $A, B, C, \cdots$ 来表示理想数．由一个整数 α 所生成的理想数 $[\alpha]$，称之为主理想数．

由 0 生成的理想数 $[0]$ 叫作零理想数，以后讨论的理想数都假定是非零理想数．

主理想数 $[1]$ 实际上就是 $R(\theta)$ 中全体整数的集合，称为单位理想数，并以 E 表示之．

以下，我们给出有关理想数的相等、相乘、因数、素理想等种种定义，并列出类似有理整数情形的若干定理，最后得到重要的理想数的唯一分解定理．但为节省篇幅，其证明过程就不在此一一给出了．

定义. $A=[\alpha_1,\cdots,\alpha_q]$ 及 $B=[\beta_1,\cdots,\beta_r]$ 为 $R(\theta)$ 上的二理想数,如果 A 中每一整数均在 B 中,而 B 中每一整数也均在 A 中时,则称它们相等,并记为 $A=B$.

定义. 设 $A=[\alpha_1,\cdots,\alpha_q]$, $B=[\beta_1,\cdots,\beta_r]$, 我们称理想数 $[\alpha_1\beta_1,\cdots,\alpha_1\beta_r,\alpha_2\beta_1,\cdots,\alpha_2\beta_r,\cdots,\alpha_q\beta_1,\cdots,\alpha_q\beta_r]$ 为 A 和 B 的乘积,记为 AB.

容易验证,乘积 AB 不依赖于 A 和 B 的表示法,即如果

$$A=[\alpha_1,\cdots,\alpha_q]=[\alpha_1',\cdots,\alpha_s'],$$
$$B=[\beta_1,\cdots,\beta_r]=[\beta_1',\cdots,\beta_t'],$$

则有

$$[\alpha_1\beta_1,\cdots,\alpha_1\beta_r,\cdots,\alpha_q\beta_1,\cdots,\alpha_q\beta_r]$$
$$=[\alpha_1'\beta_1',\cdots,\alpha_1'\beta_t',\cdots,\alpha_s'\beta_1',\cdots,\alpha_s'\beta_t'].$$

理想数的乘法满足交换律和结合律也不难验证.

由于 $EA=AE=A$, 故单位理想数 E 起着类似有理整数 1 的作用.

定义. 设 A,B 是两个理想数,如果存在理想数 C 使得

$$A=BC,$$

则称 B 可整除 A, 记为 $B|A$, 并称 B 为 A 的因子.

定理 1. 对于任一理想数 A, 一定能找到一个理想数 B, 使 $AB=[a]$, a 是一个正有理整数.

定理 2. 如果 $AB=AC$, 则有 $B=C$.

定理 3. $A|B$ 的充分必要条件是 B 中每一个数均在 A 中, 即 $B\subseteq A$.

定义. 如果一个理想数的因子只有 E 和本身, 则称为素理想数,常用 P 记之.

定理 4. 任给二理想数 $A=[\alpha_1,\cdots,\alpha_q]$ 和 $B=[\beta_1,\cdots,\beta_r]$, 则存在唯一的理想数 D, 并有性质:

1) $D|A$, $D|B$.

2) 如果 $D_1|A$, $D_1|B$, 则 $D_1|D$.

3) D 中任一数均能写成 $\alpha+\beta$ 形式, α 在 A 中, β 在 B 中.

容易验证，$D=[\alpha_1, \cdots, \alpha_q, \beta_1, \cdots, \beta_r]$，它就称为 A 和 B 的最大公因数，记为 $(A, B)=D$. 如果 $(A, B)=E$，则称 A，B 互素.

定理 5. 如果 P 为一素理想数，且 $P|AB$，$P\nmid A$，则 $P|B$.

定理 6. 任何理想数只能有有限个不同的因子.

定理 7 (理想数的唯一分解定理). 任一不同于 E 的理想数 A 可以分解为素理想数的乘积，且如果不计其排列的次序，则分解法唯一.

和有理整数类似，我们将讨论理想数的同余关系. 在讨论同余之前，先讨论理想数的基底.

设 A 是 n 次代数数域 $R(\theta)$ 的一个理想数，我们有

定理 8. 存在 A 中的 n 个数 $\alpha_1, \cdots, \alpha_n$ 使得 A 的每一个数能够唯一地表示成

$$k_1\alpha_1+\cdots+k_n\alpha_n, \tag{2}$$

这里 $k_1, \cdots, k_n$ 是有理整数. 且称此 $\alpha_1, \cdots, \alpha_n$ 为 A 的基底.

证. 由于存在正有理整数 a 和理想数 B，使

$$AB=[a],$$

因此 $aw_1, \cdots, aw_n$ 都在 A 中，这里 $w_1, \cdots, w_n$ 是 $R(\theta)$ 的一组整底，设 a_{11} 是最小的正有理整数，使得

$$\alpha_1=a_{11}w_1$$

在 A 中，因为 A 包含 $a_{11}w_1$ 和 aw_2，则包含 $k_1a_{11}w_1+k_2aw_2$，k_1, k_2 是任给的有理整数，设 a_{22} 是最小的正有理整数使得

$$\alpha_2=a_{21}w_1+a_{22}w_2$$

在 A 中，同样地对于 $i=3, \cdots, n$，设

$$\alpha_i=a_{i1}w_1+\cdots+a_{ii}w_i,$$

这里 $a_{i1}, \cdots, a_{ii}$ 是有理整数，且 a_{ii} 是最小的正整数使得 α_i 在 A 中，下面证明 $\alpha_1, \cdots, \alpha_n$ 就是所要求的 A 的一组基底.

设 $\alpha\in A$，故有有理整数 $c_1, \cdots, c_n$ 使

$$\alpha=c_1w_1+\cdots+c_nw_n,$$

则对任意的整数 c，$\alpha-c\alpha_n$ 在 A 中，因为 $c_n\geqslant a_{nn}$，用带余除法

得

$$0 \leqslant c_n - a_{nn}\left[\frac{c_n}{a_{nn}}\right] < a_{nn},$$

故 $\alpha - \left[\frac{c_n}{a_{nn}}\right]\alpha_n$ 经 $w_1, \cdots, w_n$ 表示出时，w_n 的系数为零，即有

$$\alpha - \left[\frac{c_n}{a_{nn}}\right]\alpha_n = d_1 w_1 + \cdots + d_{n-1} w_{n-1}.$$

继续讨论下去可得

$$\alpha = \left[\frac{c_n}{a_{nn}}\right]\alpha_n + \left[\frac{d_{n-1}}{a_{n-1, n-1}}\right]\alpha_{n-1} + \cdots + \left[\frac{t_1}{a_{11}}\right]\alpha_1,$$

这就证明了 A 中任一 α 可表示为 (2) 的形状. 其表示法的唯一性，是因为

$$\triangle(\alpha_1, \cdots, \alpha_n) = a_{11}^2 a_{22}^2 \cdots a_{nn}^2 \triangle(w_1, \cdots, w_n) \neq 0,$$

从而可知 $\alpha_1, \cdots, \alpha_n$ 实际上也是 $R(\theta)$ 的一组基底. 证完.

由这个定理的证明可知，存在 $R(\theta)$ 的一组基底，它同时也是 A 的基底. 由此可知 A 的任何一组基底一定也是 $R(\theta)$ 的一组基底. 而且不难验证，A 的任何两组基底的判别式必相等. 今后以 $\triangle(A)$ 表示理想数 A 的基底的判别式.

这个定理的证明还告诉我们存在 A 的一组基底 $\alpha_1, \cdots, \alpha_n$ 具有如下的形状:

$$\begin{aligned}
&\alpha_1 = a_{11} w_1,\\
&\alpha_2 = a_{21} w_1 + a_{22} w_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots,\\
&\alpha_n = a_{n1} w_1 + a_{n2} w_2 + \cdots + a_{nn} w_n.
\end{aligned} \tag{3}$$

进一步有如下定理:

定理 9. $R(\theta)$ 上的任一个理想数 A 存在一组形状如 (3) 的基底 $\alpha_1, \cdots, \alpha_n$，且可要求有理整数 a_{ij} 满足

$$0 \leqslant a_{ij} < a_{jj} \quad (1 \leqslant j < i \leqslant n).$$

证. 显然，对于 $j \neq i$ 和任意有理整数 k，

$$\alpha_1, \cdots, \alpha_{i-1}, \alpha_i - k\alpha_j, \alpha_{i+1}, \cdots, \alpha_n$$

仍是A的一组基底．于是α_n可以减去α_{n-1}的一个适当的倍数，使得w_{n-1}的系数小于$a_{n-1,n-1}$，而同时并不改变w_n的系数．类似的，可以继续减去α_{n-2}的一个适当的倍数，$\cdots$，减去α_1的一个适当的倍数．这样得到一组新的基底

$$\alpha_1, \cdots, \alpha_{n-1}, \alpha'_n = a'_{n1}w_1 + \cdots + a'_{n,n-1}w_{n-1} + a_{nn}w_n,$$
$$0 \leqslant a'_{ni} < a_{ii} \quad (i = 1, \cdots, n-1),$$

然后再对$\alpha_{n-1}, \cdots, \alpha_2$作类似的处理．便得到所需的基底．证完．

定理 9 给出的基底称为A的标准基底．

现考虑同余关系．

如果$A|[\alpha]$，以后简记为$A|\alpha$，即表示α在A中．

定义． 设α，β是$R(\theta)$中的整数，$A|\alpha-\beta$，则称α和β对模A同余．记为

$$\alpha \equiv \beta \pmod A.$$

根据这一同余关系，可以将域$R(\theta)$中的全体整数分类，使凡属于同一类的数对模A互相同余，而属于不同类的数对模A不同余．称这样的类为A的剩余类．并以$N(A)$来记不同的剩余类的个数．$N(A)$也叫理想数A的距或范数．

定理 10． 设$w_1, \cdots, w_n$为$R(\theta)$的一组整底，而$\alpha_1, \cdots, \alpha_n$为理想数$A$的一组基底，如果

$$\alpha_i = \sum_{j=1}^{n} a_{ij}w_j \qquad (i = 1, \cdots, n),$$

则$N(A) = ||a_{ij}||$．

证．因为数值$||a_{ij}||$与A的基底的选择无关，故可取$\alpha_1, \cdots, \alpha_n$为$A$的标准基底．$R(\theta)$中任一整数$\alpha = b_1w_1 + \cdots + b_nw_n$，$b_1, \cdots, b_n$是有理整数，可以减去$\alpha_n$的适当倍数，以及$\alpha_{n-1}$的适当倍数等等，使

$$\alpha \equiv a_1w_1 + \cdots + a_nw_n \pmod A, \quad 0 \leqslant a_i < a_{ii}$$
$$(i = 1, 2, \cdots, n),$$

而形如 $a_1w_1+\cdots+a_nw_n$, $0\leqslant a_i<a_{ii}$ $(i=1,\cdots,n)$ 的整数共有 $a_{11}a_{22}\cdots a_{nn}=||a_{ij}||$ 个，且其中任意两个模 A 不同余．因如不然的话，设其中两个对模 A 同余，则有

$$a_1w_1+\cdots+a_nw_n\equiv a_1'w_1+\cdots+a_n'w_n \pmod A.$$

因两端对应系数不全相同，故可设

$$a_n=a_n',\cdots,a_{n-k+1}=a_{n-k+1}',a_{n-k}>a_{n-k}' \quad (0\leqslant k\leqslant n-1),$$

则

$$(a_1-a_1')w_1+\cdots+(a_{n-k}-a_{n-k}')w_{n-k}\equiv 0 \pmod A,$$

而 $0<a_{n-k}-a_{n-k}'<a_{n-k,n-k}$, 这与 $a_{n-k,n-k}$ 的选择矛盾．证完

推论 1. 设 $\triangle$ 为域 $R(\theta)$ 的基数，$\triangle(A)$ 为 A 的基底的判别式，则

$$\triangle(A)=(N(A))^2\triangle.$$

推论 2. 对于主理想数 $[\alpha]$ 的距 $N([\alpha])$, 有

$$N([\alpha])=|N(\alpha)|.$$

此由 $\alpha w_1,\cdots,\alpha w_n$ 为 $[\alpha]$ 的基底和推论 1 即可推出．

关于素理想数，我们有：

定理 11. 若 P 为一素理想数，$P\nmid\alpha$, α 是 $R(\theta)$ 中任一整数，则有

$$\alpha^{N(P)-1}\equiv 1 \pmod P.$$

证．设 $0,\pi_1,\cdots,\pi_{N(P)-1}$ 是模 P 剩余类的代表，则 $0,\alpha\pi_1,\cdots,\alpha\pi_{N(P)-1}$ 也是各类的代表，因此

$$\alpha^{N(P)-1}\pi_1\cdots\pi_{N(P)-1}\equiv\pi_1\cdots\pi_{N(P)-1} \pmod P,$$

故得定理．证完．

定理 12. 任给素理想数 P, 一定存在有理素数 p, 使 $P|p$, 且 p 是 P 中最小的有理正整数，故是唯一确定的．

证．已知必有有理正整数 $a>1$, 使 $P|a$, 故必有有理素数 $p|a$, 使 $P|p$, 如果有正有理整数 $b<p$, 且 $P|b$, 则 $(p,b)=1$ 在 P 中，于是有 $[1]=P$, 这是不可能的．故 p 是 P 中最小的正有理整数．证完．

定理 13. $$N(AB)=N(A)N(B).$$

§6. 二次域 $R(\sqrt{m})$

我们已经证明了如果m过所有不等于1的无平方因子的整数，则 $R(\sqrt{m})$ 经过所有的二次域. 现在我们就前面各节所引入的种种定义和结果，在二次域 $R(\sqrt{m})$ 上作更具体更深入的讨论.

1. 二次域的整数和整底

二次域 $R(\sqrt{m})$ 的任一数均能表示为

$$\alpha=\frac{a+b\sqrt{m}}{2}, \tag{1}$$

其中 a, b 为有理数，α 的迹与范数各为

$$T(\alpha)=a,\ N(\alpha)=\frac{a^2-b^2m}{4}. \tag{2}$$

定理 1. 二次域 $R(\sqrt{m})$中，α 为整数的充分必要条件是：(1) 式中 a, b 都是有理整数，且适合

$$\begin{aligned}&a\equiv b\ (\mathrm{mod}\ 2),\ \text{当}\ m\equiv 1\ (\mathrm{mod}\ 4)\ \text{时},\\&a\equiv b\equiv 0\ (\mathrm{mod}\ 2),\ \text{当}\ m\equiv 2,3\ (\mathrm{mod}\ 4)\ \text{时}.\end{aligned} \tag{3}$$

证. 因在二次域中，α 为整数的充分必要条件是(2)中 $T(\alpha)$, $N(\alpha)$ 皆为有理整数. 故如果 a, b 为有理整数且 (3) 成立. 则 α 为整数.

反之，如果 α 为整数，则 a 及 $\dfrac{a^2-b^2m}{4}$ 均为有理整数，于是

$$b^2m=a^2-4\left(\frac{a^2-b^2m}{4}\right)$$

也是整数，但 m 为无平方因子的有理整数，故 b 必须为有理整数，又由

$$a^2-b^2m\equiv 0\ (\mathrm{mod}\ 4),$$

易知 (3) 成立. 证完.

定理 2. 设

$$\triangle = \begin{cases} m \\ 4m, \end{cases} \quad w = \begin{cases} \dfrac{1+\sqrt{m}}{2} & 当\ m \equiv 1 \pmod 4\ 时, \\ \sqrt{m} & 当\ m \equiv 2, 3 \pmod 4\ 时. \end{cases}$$

则$\triangle$为$R(\sqrt{m})$的基数,而 1, w 为一组整底. 又

$$1, \quad \frac{\triangle+\sqrt{\triangle}}{2}$$

也是$R(\sqrt{m})$的一组整底.

证. $m \equiv 1 \pmod 4$ 时, $\dfrac{1+\sqrt{m}}{2}$ 为整数,且

$$\frac{a+b\sqrt{m}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{m}}{2},$$

而 $m \equiv 2, 3 \pmod 4$ 时, $\sqrt{m}$ 为整数,且

$$\frac{a+b\sqrt{m}}{2} = \frac{a}{2} + \frac{b}{2}\sqrt{m},$$

故 1, w 是一组整底,又

$$\begin{vmatrix} 1 & 1 \\ \sqrt{m} & -\sqrt{m} \end{vmatrix}^2 = 4m, \quad \begin{vmatrix} 1 & 1 \\ \dfrac{1+\sqrt{m}}{2} & \dfrac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m,$$

又

$$\begin{vmatrix} 1 & 1 \\ \dfrac{\triangle+\sqrt{\triangle}}{2} & \dfrac{\triangle-\sqrt{\triangle}}{2} \end{vmatrix}^2 = \triangle.$$

而 1, $\dfrac{\triangle+\sqrt{\triangle}}{2}$ 是整数,故可推出它也是整底. 证完.

现在可以证明§4中最后的例子中 2, 3, $1 \pm \sqrt{-5}$ 都是 $R(\sqrt{-5})$ 的素数. 设2在 $R(\sqrt{-5})$ 中可分解为 $2 = \alpha\beta$, $|N(\alpha)| > 1$, $|N(\beta)| > 1$, 记 $\alpha = a + b\sqrt{-5}$, a, b 是有理整数,则 $N(\alpha) = a^2 + 5b^2 = 2$, 此乃不可能. 同理可证 3, $1 \pm \sqrt{-5}$ 也是素数.

2. 二次域的单位数

设 $\alpha = x + yw$ 是 $R(\sqrt{m})$ 的代数整数，则 α 是单位数的充分必要条件是

$$N(x + yw) = \pm 1.$$

所以只要求出适合上式的全部有理整数对 (x, y)，就得到了 $R(\sqrt{m})$ 的所有单位数。

因为

$$N(x + yw) = (x + yw)(x + yw')$$

$$= \begin{cases} \left(x + \frac{y}{2}\right)^2 - \frac{y^2}{4} m, & \text{当 } m \equiv 1 \pmod 4 \text{ 时}, \\ x^2 - y^2 m, & \text{当 } m \equiv 2, 3 \pmod 4 \text{ 时}. \end{cases}$$

故在 $m < 0$ 时，$R(\sqrt{m})$中只有有限个单位数．可设 $m = -d$，$d > 0$。

当 $m \equiv 2, 3 \pmod 4$ 时，则 $d \equiv 1, 2 \pmod 4$，在 $d > 1$ 时，

$$x^2 + y^2 d = \pm 1$$

仅有解 $x = \pm 1$，$y = 0$，此时只有单位数 ± 1；而在 $d = 1$ 时，通过对上式求解，得到四个单位数为 ± 1，$\pm i$。

当 $m \equiv 1 \pmod 4$ 时，则 $d \equiv 3 \pmod 4$，在 $d > 3$ 时，

$$(2x + y)^2 + y^2 d = 4$$

仅有解 $x = \pm 1$，$y = 0$，即只有单位数 ± 1，而在 $d = 3$ 时，易知有六个单位数 ± 1，$\pm \frac{1 + \sqrt{-3}}{2}$，$\pm \frac{1 - \sqrt{-3}}{2}$。

在 $m > 0$ 的情形，此时不定方程

$$(2x + y)^2 - y^2 m = \pm 4,$$

$$x^2 - y^2 m = \pm 1$$

均有无穷多个解．可以证明 $R(\sqrt{m})$ 中存在一个单位数 η，使凡 $R(\sqrt{m})$ 的单位数皆可表示为

$$\pm \eta^n \ (n = 0, \pm 1, \pm 2, \cdots)$$

的形式．此时 η 称为域 $R(\sqrt{m})$ 的基本单位数。

3. 二次域上理想数的标准基底

由§5定理9可知，如果 $1, w$ 为 $R(\sqrt{m})$ 的一组整底，则存在有理整数 a, b, c 满足

$$c > 0, \quad 0 \leqslant b < a,$$

使

$$a, \quad b + cw \tag{4}$$

构成 $R(\sqrt{m})$ 上理想数 A 的一组标准基底.

定理 3. 在(4)式中 $c|a$, $c|b$.

证. 由于 aw 在 A 中，故存在有理整数 x, y 使

$$aw = xa + y(b + cw).$$

由此可得 $a = yc$，故 $c|a$，又 $xa + yb = 0$，$y \neq 0$，故 $xc + b = 0$，则 $c|b$. 证完.

故理想数 A 的标准基底(4)可进一步改写为

$$cy, \quad c(v + w) \quad (c > 0, \ 0 \leqslant v < y). \tag{5}$$

定理 4. (5)式中 $y|N(v + w)$.

证. 由于 $c(v + w)w$ 在 A 中，故存在有理整数 l, n 使

$$c(v + w)w = lcy + nc(v + w),$$

而

$$c(v+w)w = -c\,(v+w)(v+w')+(v+w'+w)(v+w)c$$
$$= -\frac{N(v + w)}{y}cy + (v + T(w))(v + w)c.$$

故 $y|N(v + w)$. 证完.

推论. (5)式中 y, v 适合

$$\triangle \equiv \begin{cases} (2v + 1)^2 \pmod{4y}, & \text{若 } m \equiv 1 \pmod 4, \\ (2v)^2 \pmod{4y}, & \text{若 } m \equiv 2, 3 \pmod 4. \end{cases}$$

4. 二次域中 $[p]$ 的分解

设 p 是一有理素数，现在讨论 $R(\sqrt{m})$ 上主理想数 $[p]$ 的分解.

为此，先引入 Kronecker 符号.

定义. 设 $d \equiv 0$ 或 $1 \pmod 4$ 且非平方数. $n > 0$. Kronecker

符号 $\left(\frac{d}{n}\right)$ 之定义如下：

$$\left(\frac{d}{p}\right)=0,\qquad \text{若 } p\mid d;$$

$$\left(\frac{d}{2}\right)=\begin{cases}1, & \text{若 } d\equiv 1 \pmod 8,\\ -1, & \text{若 } d\equiv 5 \pmod 8.\end{cases}$$

$$\left(\frac{d}{p}\right)=\text{Legendre 符号}\ (p\text{ 是奇素数}, p\nmid d).$$

若 $n=\prod_{i=1}^{s} p_i$，p_i 为素数，则

$$\left(\frac{d}{n}\right)=\prod_{i=1}^{s}\left(\frac{d}{p_i}\right).$$

现在讨论$[p]$的分解. 因为

$$N(AB)=N(A)N(B),$$

故 $R(\sqrt{m})$ 上 $[p]$ 的分解显然只有下面三种可能：

(1) $[p]=P,\quad N(P)=p^2.$

(2) $[p]=PQ,\quad P\neq Q,\quad N(P)=N(Q)=p.$

(3) $[p]=P^2,\quad N(P)=p.$

这里 P, Q 均表示 $R(\sqrt{m})$ 中的素理想数.

定理 5. 情形 (1), (2), (3) 的成立，当且仅当 $\left(\frac{\triangle}{p}\right)=-1$, $+1$, 0. 此处$\triangle$为 $R(\sqrt{m})$ 的基数，$\left(\frac{\triangle}{p}\right)$ 为 Kronecker 符号[1].

证. 设 $P\mid[p]$，$N(P)=p$，即 (2)、(3) 两种情形时，设 cy, $c(v+w)$ 为素理想数 P 的标准基底，则

$$N(P)=c^2y=p.$$

故 $c=1$，$y=p$，又因

$$\triangle\equiv\begin{cases}(2v+1)^2 \pmod{4p}, & \text{当 } m\equiv 1 \pmod 4 \text{ 时},\\ (2v)^2 \pmod{4p}, & \text{当 } m\equiv 2, 3 \pmod 4 \text{ 时},\end{cases}$$

---

1) 容易验证 $\triangle\equiv 0$ 或 $1 \pmod 4$，且 $\triangle$ 非平方数.

所以得到 $\left(\frac{\triangle}{p}\right)=1$ 或 0.

反之,若 $\left(\frac{\triangle}{p}\right)=1$ 或 0,先考虑 $p\neq 2$ 的情形.

1) 如果 $\left(\frac{\triangle}{p}\right)=1$, 则存在 a, $p\nmid a$, 使 $\triangle\equiv a^2 \pmod p$, 于是

$$
\begin{aligned}
&[p, a+\sqrt{\triangle}][p, a-\sqrt{\triangle}] \\
&\quad=[p^2, p(a+\sqrt{\triangle}), p(a-\sqrt{\triangle}), a^2-\triangle] \\
&\quad=[p]\left[p, a+\sqrt{\triangle}, a-\sqrt{\triangle}, \frac{a^2-\triangle}{p}\right] \\
&\quad=[p]\left[p, a+\sqrt{\triangle}, 2a, \frac{a^2-\triangle}{p}, 1\right]=[p],
\end{aligned}
$$

又

$$[p, a+\sqrt{\triangle}]\neq[p, a-\sqrt{\triangle}],$$

不然有

$$
\begin{aligned}
[p, a+\sqrt{\triangle}]&=[p, a-\sqrt{\triangle}] \\
&=[p, 2a, a+\sqrt{\triangle}]=[1],
\end{aligned}
$$

此乃不可能. 而且 $[p, a\pm\sqrt{\triangle}]\neq[1]$; 否则有

$$[p, a+\sqrt{\triangle}]=[p, a-\sqrt{\triangle}]=[1].$$

2) 如果 $\left(\frac{\triangle}{p}\right)=0$, 则 $p\mid\triangle$, 于是

$$[p, \sqrt{\triangle}]^2=[p^2, p\sqrt{\triangle}, \triangle]=[p]\left[p, \sqrt{\triangle}, \frac{\triangle}{p}\right].$$

而 $\triangle=m$ 或 $4m$, $p\neq 2$, m 无平方因子,故 $\left(p, \frac{\triangle}{p}\right)=1$, 所以

$[p]=[p, \sqrt{\triangle}]^2$.

其次,考虑 $p=2$ 的情形. 因为 $\left(\frac{\triangle}{2}\right)\neq -1$, 故必须 $m\equiv 2, 3 \pmod 4$ 或 $m\equiv 1 \pmod 4$, $\triangle=m$, 后者推出 $m\equiv 1 \pmod 8$, 与前面一样,可证:

3) 当 $m\equiv 2 \pmod 4$ 时, $\left(\frac{\triangle}{2}\right)=0$, 而 $[2]=[2, \sqrt{m}]^2$;

4)当 $m \equiv 3 \pmod 4$ 时，仍有 $\left(\frac{\triangle}{2}\right)=0$，而

$$[2, 1+\sqrt{m}]^2 = [4, 2+2\sqrt{m}, 1+2\sqrt{m}+m]$$
$$= [4, 2+2\sqrt{m}, m-1]$$
$$= [2]\left[2, 1+\sqrt{m}, \frac{m-1}{2}\right] = [2];$$

5) 当 $m \equiv 1 \pmod 8$ 时，$\left(\frac{\triangle}{2}\right)=1$，此时

$$\left[2, \frac{1+\sqrt{m}}{2}\right]\left[2, \frac{1-\sqrt{m}}{2}\right]$$
$$= [2]\left[2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}, \frac{1-m}{8}\right]$$
$$= [2]\left[2, \frac{1+\sqrt{m}}{2}, 1, \frac{1-m}{8}\right] = [2].$$

而 $\left[2, \frac{1+\sqrt{m}}{2}\right] \neq \left[2, \frac{1-\sqrt{m}}{2}\right]$，且 $\left[2, \frac{1\pm\sqrt{m}}{2}\right] \neq [1]$，此时 [2] 分解为二个不同的素理想数的乘积．证完．

5. 欧氏域

定义． 如果对 $R(\sqrt{m})$ 中任意二个整数 $\xi, \eta(\eta \neq 0)$，存在整数 κ 与 λ，使

$$\xi = \kappa\eta + \lambda, \qquad |N(\lambda)| < |N(\eta)|, \tag{6}$$

则该域称为欧几里得域，简称欧氏域．

显然，下面的定义与之等价．

定义． 若对 $R(\sqrt{m})$ 中任意一数 δ，必存在一整数 κ 使

$$|N(\delta-\kappa)| < 1, \tag{7}$$

则 $R(\sqrt{m})$ 称为欧氏域．

如果 $R(\sqrt{m})$ 为欧氏域，则 $R(\sqrt{m})$ 中整数的唯一分解定理成立．即有下面定理．

定理 6． $R(\sqrt{m})$ 为欧氏域．以 π_j，π_j' 表示 $R(\sqrt{m})$ 中的素

数．设 α 是 $R(\sqrt{m})$ 中的任一整数，$|N(\alpha)|>1$，若

$$\alpha=\pi_1\cdots\pi_r=\pi_1'\cdots\pi_s' \qquad (r\geqslant 1, s\geqslant 1),$$

则有 $r=s$，且可适当调整次序，使 π_i 是 π_i' 的结合数($i=1,\cdots,s$)．

由于(6)成立．完全可以仿照有理整数的唯一分解定理的证明步骤来证明．

定理 7．仅有五个二次虚欧氏域，即

$$R(\sqrt{-1}), R(\sqrt{-2}), R(\sqrt{-3}), R(\sqrt{-7}), R(\sqrt{-11}).$$

证．1) 若 $m\equiv 2, 3 \pmod 4$，取 $\delta=t+s\sqrt{m}$，$\kappa=x+y\sqrt{m}$，则(7)式变为对任意一对有理数 t, s 存在有理整数 x, y 使

$$|(t-x)^2-m(s-y)^2|<1, \tag{8}$$

若取 $t=s=\frac{1}{2}$，则由(8)可得

$$\frac{1}{4}+|m|\frac{1}{4}\leqslant|(t-x)^2-m(s-y)^2|<1,$$

故 $|m|<3$，即 $m=-1, -2$．

现设 $m=-1, -2$，因为对任何有理数 t, s，恒有有理整数 x, y 使

$$|t-x|\leqslant\frac{1}{2}, \quad |s-y|\leqslant\frac{1}{2}.$$

故

$$|(t-x)^2-m(s-y)^2|\leqslant\frac{1}{4}+|m|\frac{1}{4}<1.$$

所以 $R(\sqrt{-1})$，$R(\sqrt{-2})$ 为欧氏域．

2) 若 $m\equiv 1 \pmod 4$，取

$$\delta=t+s\sqrt{m}, \quad \kappa=x+\frac{1}{2}y(1+\sqrt{m}),$$

利用(7)得

$$\left|\left(t-x-\frac{1}{2}y\right)^2-m\left(s-\frac{1}{2}y\right)^2\right|<1.$$

取 $t=s=\frac{1}{4}$，则得

$$\frac{1}{16}+\frac{1}{16}|m|\leqslant\left|\left(t-x-\frac{1}{2}y\right)^2-m\left(s-\frac{1}{2}y\right)^2\right|<1,$$

故 $|m|<15$. 所以当 $m\equiv 1\pmod 4$ 时，仅可能有三个虚欧氏域 $R(\sqrt{-3})$，$R(\sqrt{-7})$，$R(\sqrt{-11})$.

因为对任何有理数 t，s，总有有理整数 x，y，使

$$|2s-y|\leqslant\frac{1}{2},\qquad\left|t-x-\frac{1}{2}y\right|\leqslant\frac{1}{2},$$

于是，当 $m=-3,\ -7,\ -11$ 时，

$$\left|\left(t-x-\frac{1}{2}y\right)^2-m\left(s-\frac{1}{2}y\right)^2\right|\leqslant\frac{1}{4}+\frac{1}{16}|m|\leqslant\frac{15}{16}<1.$$

这表明 $m=-3,\ -7,\ -11$ 时，$R(\sqrt{m})$ 是欧氏域. 证完.

定理 8. 欧氏域 $R(\sqrt{m})$ 的素数 π 整除唯一的一个有理素数 p.

证. 由于 $\pi|N(\pi)=\pi\pi'$，$\pi||N(\pi)|$，故存在有理正整数被 π 整除. 设 z 是被 π 整除的最小有理正整数，则 z 必定是一个有理素数p. 否则，设 $z=z_1z_2$，$1<z_1$，$z_2<z$，则有 $\pi|z_1$ 或 $\pi|z_2$，这均与 z 的假设矛盾.

如果还有素数 $p'\neq p$，$\pi|p'$，则由 $(p,p')=1$ 得到 $\pi|1$，这是不可能的. 证完.

定理 9. 欧氏域 $R(i)$ 的素数是

1) $1+i$ 和它的结合数.

2) 有理素数 $q(q\equiv 3\pmod 4)$ 和它的结合数.

3) 有理素数 $p(p\equiv 1\pmod 4)$ 的因数

$$a+bi,\quad N(a+bi)=p.$$

证. 设 $\pi=a+bi$，则由定理 8 知存在唯一的有理素数 p，使 $\pi|p$. 设 $\pi\lambda=p$，则 $N(\pi)N(\lambda)=p^2$. 故或者 $N(\lambda)=1$，此时 λ 是一个单位数，π 是一个 p 的结合数；或者 $N(\pi)=a^2+b^2=p$. 如 $p=2$，则 $a=b=1$，故 $1+i$ 和它的结合数是 $R(i)$ 的素数.

1) 已证明. 如果 $p \equiv 3 \pmod 4$, 则 $a^2 + b^2 = p$ 不可能. 故 $p \equiv 3 \pmod 4$ 和它的结合数是 $R(i)$ 的素数. 2) 已证明. 如果 $p \equiv 1 \pmod 4$, 则 $\left(\frac{-1}{p}\right) = 1$, 故存在有理整数 x, 使 $p | x^2 + 1 = (x+i)(x-i)$, 此时, 显然 p 不是素数. 否则, 有 $p | x + i$ 或 $p | x - i$, 易知这两种情形均不可能. 故 $p = \pi\lambda$, 这里 $\pi = a + bi$, $\lambda = a - bi$, 且 $N(\pi) = a^2 + b^2$, 这就证明了 3). 证完.

§7. 属于不同域的理想数

设 $F = R(\theta)$, $F' = R(\theta')$ 是 R 的两个扩域,且满足 $F \subseteq F'$, 现在考虑 F 中的整数 $\alpha_1, \cdots, \alpha_q$ 在 F 中生成的理想数 $A = [\alpha_1, \cdots, \alpha_q]_F$ 和在 F' 中生成的理想数 $A' = [\alpha_1, \cdots, \alpha_q]_{F'}$ 之间的关系.

定理 1. $A = [\alpha_1, \cdots, \alpha_q]_F = A' \cap F$.

证. 设 $\alpha \in A$, 显然有 $\alpha \in A'$, $\alpha \in F$, 故 $\alpha \in A' \cap F$.

反之, 设 $\alpha \in A'$ 和 $\alpha \in F$, 则

$$\alpha = \sum_{j=1}^{q} \lambda_j \alpha_j, \qquad \lambda_j \in F' (j = 1, \cdots, q).$$

假如 $(F'|F) = m$, 则

$$\alpha = \sum_{j=1}^{q} \lambda_j^{(i)} \alpha_j \qquad (i = 1, \cdots, m), \tag{1}$$

这里 $\lambda_j^{(i)}$ 表示 λ_j 在 F 上的第 i 个共轭 $(i = 1, \cdots, m; j = 1, \cdots, q)$.

把 (1) 中的 m 个式子的两端各自相乘得

$$\alpha^m = \prod_{i=1}^{m} \sum_{j=1}^{q} \lambda_j^{(i)} \alpha_j = \sum_{\substack{0 \leqslant i_1, \cdots, i_q \leqslant m \\ i_1 + \cdots + i_q = m}} b_{i_1, \cdots, i_q} \alpha_1^{i_1} \cdots \alpha_q^{i_q}.$$

应用对称多项式定理知数 $b_{i_1, \cdots, i_q} \in F$, 因此

$$\alpha^m \in A^m.$$

由 $A^m | \alpha^m$, 可推出 $A | \alpha$, 即 $\alpha \in A$. 证完.

定理 2. 设 F, F_1 是两个数域，均包含有数 $\alpha_1, \cdots, \alpha_q, \beta_1, \cdots, \beta_r$. 如果

$$[\alpha_1, \cdots, \alpha_q]_F = [\beta_1, \cdots, \beta_r]_F,$$

则

$$[\alpha_1, \cdots, \alpha_q]_{F_1} = [\beta_1, \cdots, \beta_r]_{F_1}.$$

证. 考虑一个公共扩域 F'，它包含 F 也包含 F_1，则有

$$[\alpha_1, \cdots, \alpha_q]_{F'} = [\beta_1, \cdots, \beta_r]_{F'}.$$

由定理 1 知道有

$$[\alpha_1, \cdots, \alpha_q]_{F_1} = [\alpha_1, \cdots, \alpha_q]_{F'} \cap F_1,$$

$$[\beta_1, \cdots, \beta_r]_{F_1} = [\beta_1, \cdots, \beta_r]_{F'} \cap F_1,$$

故 $[\alpha_1, \cdots, \alpha_q]_{F_1} = [\beta_1, \cdots, \beta_r]_{F_1}$. 证完.

于是我们可以定义在不同的两个域中理想数的相等.

设理想数 $A = [\alpha_1, \cdots, \alpha_q]_F$ 和理想数 $A_1 = [\beta_1, \cdots, \beta_r]_{F_1}$ 分别是 F 和 F_1 的两个理想数. 如果存在域 F', $F' \supseteq F$, $F' \supseteq F_1$, 使得

$$[\alpha_1, \cdots, \alpha_q]_{F'} = [\beta_1, \cdots, \beta_r]_{F'}.$$

则我们称 A 和 A_1 相等，并记为 $A = A_1$.

同样地，我们可以定义属于不同域的两个理想数的乘积和最大公因数.

设 $A = [\alpha_1, \cdots, \alpha_q]_F$, $B = [\beta_1, \cdots, \beta_r]_{F_1}$. $F' \supseteq F$, $F' \supseteq F_1$, 则我们定义

$$[\alpha_1\beta_1, \cdots, \alpha_1\beta_r, \cdots, \alpha_q\beta_1, \cdots, \alpha_q\beta_r]_{F'}$$

和

$$[\alpha_1, \cdots, \alpha_q, \beta_1, \cdots, \beta_r]_{F'}$$

分别为 A 和 B 的乘积与 A 和 B 的最大公因数，并记为 AB 和 (A, B).

不难证明以上定义均与扩域 F' 的选择无关.

下面，我们再引进理想数的共轭和它们的乘积的概念.

定义. 设 $F = R(\theta)$ 是一个 n 次扩域. $A = [\alpha_1, \cdots, \alpha_q]_F$

是F的一个理想数．把A中的每一个数换成它的第i个共轭数所成的集是$F^{(i)}=F(\theta^{(i)})$的一个理想数，叫A的第i个共轭理想数，记为$A^{(i)}(i=1,\cdots,n)$，所有共轭理想数的乘积，记为$n(A)=A^{(1)}\cdots A^{(n)}$．如果$F=R(\theta)$是$R$上的正规扩域，则有$n(A)=[N(A)]$．

§8. 素理想数的一些性质

本节考虑$F=R(\theta)$的素理想数P的一些性质．

定理 1．设P是一个素理想数．则$R(\theta)$中的全体整数模P的剩余类对模P的加法和乘法成域．且$N(P)=p^f$，这里p是有理素数，且$P|p$，f叫做P的次数．

证．显然模P剩余类对模P的加法和乘法组成一个有单位元的交换环．因为由$\alpha\beta\equiv 0\ (\bmod P)$可以推出$\alpha\equiv 0\ (\bmod P)$或$\beta\equiv 0\ (\bmod P)$，故这个环是整环．因为模$P$的剩余类的个数$N(P)$有限，所以构成一个有限域．设这个域的特征是素数$p$，则

$$N(P)=p^f.$$

又因为

$$P|N(P)=p^f,$$

故

$$P|p.$$

证完．

定理 2．设P是一个素理想数，则$R(\theta)$中的全体整数模P的剩余类组成的有限域中，存在一个阶为$N(P)-1$的元β，且对任一整数α有

$$\alpha^{N(P)}\equiv\alpha\ (\bmod P).$$

这是有限域中一个熟知的结果．其证明就不在这里列出了．

推论．设a是一个有理整数，α是$R(\theta)$中的一个整数，则$\alpha\equiv a\ (\bmod P)$的充分必要条件是

$$\alpha^p\equiv\alpha\ (\bmod P).$$

证．设　　$P|p,\ \alpha\equiv a\ (\bmod P),$

由

$$a^p \equiv a \pmod{p},$$

得

$$a^p \equiv a \pmod{P},$$

故

$$\alpha^p \equiv \alpha \pmod{P}.$$

反之，设 $\alpha^p \equiv \alpha \pmod{P}$，而 $x^p \equiv x \pmod{P}$ 恰有 p 个根 $0, 1, \cdots, p-1$ 模 P，故 $\alpha \equiv a \pmod{P}$. 证完.

下面，我们给出重要的 Dedekind 定理

定理 3. 设 $F = R(\theta)$ 是一个 n 次域，P 是其中的一个素理想数，p 是一个有理素数，$\triangle$ 是域 F 的基数. 则

$$p \equiv 0 \pmod{P^2}$$

的充分必要条件是 $p \mid \triangle$.

证. 由于充分性的证明太长，限于篇幅，我们仅给出定理的必要性的证明.

设 α 是 F 的一个整数，则有

$$T(\alpha^p) \equiv (T(\alpha))^p \pmod{p}, \tag{1}$$

设 $w_1, \cdots, w_n$ 是 $R(\theta)$ 的一组整底，于是有

$$\triangle = \triangle(w_1, \cdots, w_n) = |T(w_i w_j)|, \tag{2}$$

所以 (1), (2) 给出

$$\triangle(w_1, \cdots, w_n) \equiv \triangle(w_1^p, \cdots, w_n^p) \pmod{p}, \tag{3}$$

因为 $P^2 \mid p$，故可设 $[p] = P^\lambda A$，$(P, A) = [1]$，$\lambda \geqslant 2$. 由此推出 $R(\theta)$ 中存在整数 β 满足

$$\beta \equiv 0 \pmod{P^{\lambda-1}A}, \qquad \beta \not\equiv 0 \pmod{P^\lambda A}. \tag{4}$$

利用 $\lambda \geqslant 2$ 和 (4) 可以推出对有理素数 p 有

$$\beta^p \equiv 0 \pmod{p} \text{ 和 } p \nmid \beta.$$

再令

$$\beta = c_1 w_1 + \cdots + c_n w_n$$

其中 $c_1, \cdots, c_n$ 是不全部被 p 整除的有理整数，则有

$$c_1(w_1^{(i)})^p + \cdots + c_n(w_n^{(i)})^p \equiv 0 \pmod{p} \quad (i = 1, \cdots, n),$$

于是

$$\triangle(w_1^p, \cdots, w_n^p) \equiv 0 \pmod{p}.$$

再由 (3) 即得 $p|\triangle$. 证完.

§9. [p] 的 分 解

仍设 $F = R(\theta)$ 是一个 n 次代数数域, p 是一个有理素数. 本节主要研究 F 中主理想数 $[p]$ 的分解.

定理 1. 设 $F = R(\theta)$, $f(x)$ 是 R 上首项系数为 1 的 n 次整系数不可约多项式. $f(\theta) = 0$, 且设

$$f(x) \equiv f_1^{e_1}(x)\cdots f_r^{e_r}(x) \pmod p,$$
$$r \geqslant 1, e_i \geqslant 1 \quad (i = 1, \cdots, r), \tag{1}$$

这里 $f_i(x)$ 是模 p 不可约多项式, $f_i(x)$ 的次数为 $n_i > 0$, 且

$$\text{index}(\theta) \not\equiv 0 \pmod p, \tag{2}$$

则

$$[p] = P_1^{e_1}\cdots P_r^{e_r}.$$

这里 $P_i = [p, f_i(\theta)]$, 是次数为 n_i 的素理想数 $(i = 1, \cdots, r)$.

证明这个定理需要下面几个引理.

引理 1. 在定理 1 的假设条件下, p^n 个数

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}, \quad b_i = 0, 1, \cdots, p-1$$
$$(i = 0, 1, \cdots, n-1)$$

组成环 $I_p(\theta)$ 的一组完全剩余系. 这里 $I_p(\theta)$ 表示 $R(\theta)$ 中全体整数模 $[p]$ 的剩余类环.

证. 环 $I_p(\theta)$ 有 $N([p]) = p^n$ 个元素. 故只需证明由

$$\sum_{i=0}^{n-1} a_i\theta^i \equiv 0 \pmod p, \ a_i\text{是有理整数}\ (i = 0, 1, \cdots, n-1) \tag{3}$$

可以推出

$$a_i \equiv 0 \pmod p \qquad (i = 0, 1, \cdots, n-1).$$

设 $w_1, \cdots, w_n$ 是 $R(\theta)$ 的一组整底, 且

$$\theta^i = \sum_{j=1}^{n} c_{ij}w_j \qquad (i = 0, 1, \cdots, n-1),$$

则由 (2) 知道 $|c_{ij}| \not\equiv 0 \pmod p$,故由 (3) 得

$$\sum_{i=0}^{n-1}\sum_{j=1}^{n} a_i c_{ij} w_j = \sum_{j=1}^{n} w_j \sum_{i=0}^{n-1} a_i c_{ij} \equiv 0 \pmod p.$$

因为 $w_1, \cdots, w_n$ 是一组整底. 推出

$$\sum_{i=0}^{n-1} c_{ij} a_i \equiv 0 \pmod p \qquad (j = 1, \cdots, n),$$

利用 $|c_{ij}| \not\equiv 0 \pmod p$, 从上式即可推出

$$a_i \equiv 0 \pmod p \qquad (i = 0, 1, \cdots, n-1).$$

证完.

引理 2. 设 $g(x)$ 是有理整系数的多项式, 且模 p 不可约, 则在定理 1 的假设条件下. 理想数

$$P = [g(\theta), p]$$

或者是 $[1]$, 或者是一个素理想数.

证. 如果 $P \neq [1]$, 那么只需证明, 对任意整数 α, β, 如果 $\alpha\beta \equiv 0 \pmod P$, $\alpha \not\equiv 0 \pmod P$, 可以推出 $\beta \equiv 0 \pmod P$.

由引理 1 得, $\alpha \equiv a(\theta) \pmod p$, $\beta \equiv b(\theta) \pmod p$. 这里 $a(x)$, $b(x)$ 是次数不超过 $n-1$ 的有理整系数多项式. 因 $g(x)$ 是模 p 不可约的, $a(\theta) \not\equiv 0 \pmod P$, 则 $a(x)$ 和 $g(x)$ 是模 p 互素的. 故存在模 p 的多项式 $m(x)$ 和 $n(x)$ 使得

$$a(x)m(x) + g(x)n(x) \equiv 1 \pmod p,$$

故有

$$a(x)m(x)b(x) + g(x)n(x)b(x) \equiv b(x) \pmod p.$$

将 $x = \theta$ 代入上式, 可得

$$\beta \equiv b(\theta) \equiv 0 \pmod P.$$

证完.

引理 3. 定理 1 中的 $[f_i(\theta), p] \neq [1] \quad (i = 1, \cdots, r)$.

证. 如果 $[f_i(\theta), p] = [1] \quad (1 \leqslant i \leqslant r)$, 不失一般, 设 $[f_1(\theta), p] = [1]$, 在 (1) 中令 $x = \theta$, 可得

$$h(\theta) = f_2^{e_2}(\theta) \cdots f_r^{e_r}(\theta) \equiv 0 \pmod p.$$

因为 $h(\theta)$ 含 θ 的次数小于 n. 由引理 1 知这是不可能的. 证

完.

引理 4. 如果 $g(x)$, $h(x)$ 是模 p 互素的,则

$$[g(\theta), h(\theta), p] = [1].$$

证. 存在 $a(x)$ 和 $b(x)$ 使得

$$a(x)g(x) + b(x)h(x) \equiv 1 \pmod{p},$$

因此

$$a(\theta)g(\theta) + b(\theta)h(\theta) \equiv 1 \pmod{p},$$

故 $1 \in [g(\theta), h(\theta), p]$, 即得 $[g(\theta), h(\theta), p] = [1]$. 证完.

现在我们转来证明定理 1.

证. 由引理 2 和引理 3, 可设

$$[f_i(\theta)] = P_iA_i, \quad [p] = P_iB_i \quad (i = 1, \cdots, r),$$

这里 $(A_i, B_i) = [1]$, P_i 是一个素理想数. 由 (1) 可得

$$0 = f(\theta) \equiv f_1^{e_1}(\theta)\cdots f_r^{e_r}(\theta) \pmod{p},$$

即

$$P_1^{e_1}\cdots P_r^{e_r}A_1^{e_1}\cdots A_r^{e_r} \equiv 0 \pmod{P_1B_1}.$$

因为 $(A_1, B_1) = [1]$, 由上式可得

$$P_1^{e_1}\cdots P_r^{e_r}A_2^{e_2}\cdots A_r^{e_r} \equiv 0 \pmod{P_1B_1},$$

把上式 $\bmod P_1B_1$ 换成 $\bmod P_2B_2$ 后可推出

$$P_1^{e_1}\cdots P_r^{e_r}A_3^{e_3}\cdots A_r^{e_r} \equiv 0 \pmod{P_2B_2}.$$

如此继续下去可得

$$P_1^{e_1}\cdots P_r^{e_r} \equiv 0 \pmod{p},$$

因此

$$[p] = P_1^{d_1}\cdots P_r^{d_r}, \quad e_i \geqslant d_i \geqslant 0 \quad (i = 1, \cdots, r). \tag{4}$$

从 (4) 可以推出

$$f_1^{d_1}(\theta)\cdots f_r^{d_r}(\theta) \equiv 0 \pmod{p}. \tag{5}$$

由引理 1 知由 (5) 可推出

$$\sum_{i=1}^{r} n_id_i \geqslant n,$$

但因

$$\sum_{i=1}^{r} n_ie_i = n, \quad e_i \geqslant d_i,$$

这就证明了 $d_i = e_i$ $(i=1, \cdots, r)$

对于任意一个整数 α，由

$$\alpha \equiv a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \pmod{[p]}$$

可推得

$$\alpha \equiv \langle b_0\rangle_p + \langle b_1\rangle_p\theta + \cdots + \langle b_{n_i-1}\rangle_p\theta^{n_i-1} \pmod{P_i},$$

而 p^{n_i} 个整数 $b_0 + b_1\theta + \cdots + b_{n_i-1}\theta^{n_i-1}$($b_i = 0, 1, \cdots, p-1$; $i = 0, 1, \cdots, n_i - 1$) 对模 P_i 是互不同余的. 对此，只需证明从

$$a_0 + a_1\theta + \cdots + a_{n_i-1}\theta^{n_i-1} \equiv 0 \pmod{p_i}$$

可以推出 $p|a_i$($i = 0, 1, \cdots, n_i - 1$). 否则，存在一个 j, $p\nmid a_j$. 则 $g(x) = a_0 + a_1x + \cdots + a_{n_i-1}x^{n_i-1}$ 与 $f_i(x)$ 模 p 互素，由引理 4 知 $[g(\theta), f_i(\theta), p] = [1] \subseteq P_i$，故得 $P_i = [1]$，这不可能. 所以 $N(P_i) = p^{n_i}$ $(i = 1, \cdots, r)$. 证完.

设 p 是一个有理素数，且

$$[p] = P_1^{e_1}\cdots P_r^{e_r},$$

这里素理想数 P_i 的次数是 f_i，则

$$N([p]) = N(P) = p^n = N(P_1)^{e_1}\cdots N(P_r)^{e_r} = p^{\sum_{i=1}^{r} e_if_i},$$

因此

$$n = \sum_{i=1}^{r} e_if_i. \tag{6}$$

如果 $F = R(\theta)$ 是一个 R 的正规扩域，A 是 F 的任一个理想数. 则由前面给出的结果 $n(A) = [N(A)]$，可以证明下述定理.

定理 2. 设 p 是一个有理素数，在正规扩域 $F = R(\theta)$ 中，p 可分解为

$$[p] = (P^{(j_1)}\cdots P^{(j_r)})^e \quad 1 \leqslant j_1 < \cdots < j_r \leqslant n, \tag{7}$$

且

$$n = rfe. \tag{8}$$

这里 $n = (F|R)$，素理想数 $P|p$，$N(P) = p^f$. r 是 $P = P^{(1)}, \cdots, P^{(n)}$ 中不同的素理想数的个数. 其 r 个不同的素理想数设为 $P^{(j_1)}, \cdots, P^{(j_r)}$.

证. 设 $P|p$, P 是素理想数, 因为 $n(P)=[N(p)]$, 故由 $N(P)=p^f$ 得 $n(P)=[p]^f$, 即

$$P^{(1)}\cdots P^{(n)}=[p]^f.$$

由理想数的唯一分解定理,故可设

$$[p]=(P^{(j_1)})^{e_{j_1}}\cdots(P^{(j_r)})^{e_{j_r}},\quad e_{j_t}\geqslant 1\quad(t=1,\cdots,r).$$

这里不失一般性,可设 $P=P^{(1)}=P^{(j_1)}$, 因为

$$R(\theta)=R(\theta^{(j)})\qquad(j=1,\cdots,n),$$

故存在域 F 的自同构 $\sigma_t(\theta)=\theta^{(t)}$ $(1<t\leqslant n)$, 它保持 R 的数不变,而使 $\sigma_t(P^{(j_1)})=P^{(j_s)}$ $(1<s\leqslant r)$. 因此又得

$$[p]=(P^{(j_s)})^{e_{j_1}}(P^{(i_2)})^{e_{j_2}}\cdots(P^{(i_r)})^{e_{j_r}},$$

$i_2,\cdots,i_r$ 是数 $j_1,\cdots,j_{s-1},j_{s+1},\cdots,j_r$ 的某一个排列. 由理想数的唯一分解定理得 $e_{j_s}=e_1=e$ $(s=2,\cdots,r)$. 即得(7)式.

又因在正规扩域 $R(\theta)$ 中,如果 $w_1,\cdots,w_n$ 是一组整底,则 $w_1^{(j)},\cdots,w_n^{(j)}$ 也是一组整底,故有

$$N(P)=N(P^{(i)})=p^f(i=1,\cdots,n).$$

再由(6)即得(8)式. 证完.

§10. 在分圆域上 $[p]$ 的分解

设 $m>1$, ξ_m 是 m 次本原单位根,为不失一般性,设 $\xi_m=e^{2\pi i/m}$, 域 $R(\xi_m)$ 叫 m 阶分圆域. 本节主要证明如下定理.

定理 1. 域 $R(\xi_m)$ 是 R 的 $\varphi(m)$ 次正规扩域. ξ_m 的共轭是 $\varphi(m)$ 个数 ξ_m^i, 这里 $(i,m)=1$, $R(\xi_m)$ 的基数仅被 m 的素因子所整除. 数 $1,\xi_m,\cdots,\xi_m^{\varphi(m)-1}$ 组成 $R(\xi_m)$ 的一组整底.

证明这个定理之前,首先证明:

引理 1. 设 $R(\theta)$, $R(\rho)$ 是 R 的两个扩张,使得

1) $(R(\theta,\rho)|R(\rho))=(R(\theta)|R)$. (因此, $(R(\theta,\rho)|R)=(R(\theta)|R)(R(\rho)|R)$).

2) $(\triangle(R(\theta)),\ \triangle(R(\rho)))=1$, 这里 $\triangle(R(\theta))$ 与 $\triangle(R(\rho))$ 分别表示域 $R(\theta)$ 和 $R(\rho)$ 的基数.

3) $w_1, \cdots, w_m$ 是 $R(\theta)$ 的一组整底，且 $\eta_1, \cdots, \eta_s$ 是 $R(\rho)$ 的一组整底。

那么，ms 个数 $\eta_i w_j$ $(i=1, \cdots, s; j=1, \cdots, m)$ 构成域 $R(\theta,\rho)$的一组整底.

证. $\eta_i w_j (i=1,\cdots,s; j=1,\cdots,m)$ 是 $R(\theta,\rho)$在R上的一组由整数构成的基底. 则每一个 $R(\theta,\rho)$ 中的整数 α 可表示为

$$\alpha=\sum_{i=1}^{s}\sum_{j=1}^{m} c'_{ij}\eta_i w_j,\ c'_{ij}\in R\ (i=1,\cdots,s; j=1,\cdots,m).$$

由 § 3 定理 5，可设

$$c'_{ij}=\frac{d_{ij}}{\triangle}, \triangle=\triangle\ \ (\eta_1 w_1, \cdots, \eta_s w_m),$$

d_{ij} 是有理整数. 因此，如果我们能够证明对于任一个有理素数 p，由同余式

$$\sum_{i=1}^{s}\sum_{j=1}^{m} c_{ij}\eta_i w_j \equiv 0 \pmod p,\quad c_{ij}\text{ 是有理整数} \tag{1}$$

推出 $p|c_{ij}$ $(i=1,\cdots,s; j=1,\cdots,m)$. 便证明了引理 1.

设

$$\sum_{j=1}^{m} c_{ij}w_j=\alpha_i,\qquad \sum_{i=1}^{s} c_{ij}\eta_i=\beta_j.$$

并设$\alpha_i\eta_i$ 和 $\alpha_i\eta_i^{(e)}(e=1,\cdots,s)$ 在 $R(\theta)$ 上共轭，由条件 1) 知 ρ 在$R(\theta)$上和 ρ 在R 上的定义多项式相同，因此 $\eta_i^{(e)}$ 与 η_i 在R 上也共轭. 类似地，如设 $\beta_j w_j$ 和 $\beta_j w_j^{(r)}$ $(r=1,\cdots,m)$ 在 $R(\rho)$ 上共轭，则 w_j, $w_j^{(r)}$ 在R上也共轭. 故由 (1) 式分别对 $R(\theta)$ 和 $R(\rho)$ 取共轭，可推出

$$\sum_{i=1}^{s}\alpha_i\eta_i^{(e)}\equiv\sum_{j=1}^{m}\beta_j w_j^{(r)}\equiv 0 \pmod p$$
$$(e=1,\cdots,s; r=1,\cdots,m). \tag{2}$$

再由 (2) 推出

$$\alpha_i\sqrt{\triangle(R(\rho))}\equiv\beta_j\sqrt{\triangle(R(\theta))}\equiv 0 \pmod p$$
$$(i=1,\cdots,s; j=1,\cdots,m),$$

由

$$\alpha_i\sqrt{\triangle(R(\rho))} \equiv 0 \pmod p,$$

得

$$\alpha_i \triangle(R(\rho)) = p\lambda,$$

λ 是一个代数整数. 故再由

$$\sum_{j=1}^{m} c_{ij} \triangle(R(\rho))w_j \equiv 0 \pmod p$$

推出

$$c_{ij} \triangle(R(\rho)) \equiv 0 \pmod p.$$

同理可得

$$c_{ij} \triangle(R(\theta)) \equiv 0 \pmod p.$$

以上 $i=1,\cdots,s;\ j=1,\cdots,m$. 由引理的条件 2) 推出

$$c_{ij} \equiv 0 \pmod p \quad (i=1,\cdots,s;\ j=1,\cdots,m).$$

证完.

定理 1 的证明. 我们对 m 的不同的素因数的个数用归纳法. 先证 $m=p^t$ 的情形. 此时 ξ_{p^t} 满足方程

$$\begin{aligned}\Psi(x) &= \frac{x^{p^t}-1}{x^{p^{t-1}}-1}\\ &= (x^{p^{t-1}})^{p-1} + (x^{p^{t-1}})^{p-2} + \cdots + x^{p^{t-1}} + 1 = 0. \quad (3)\end{aligned}$$

我们令 $\xi_{p^t}=\xi$, 因为 ξ^k, $(k, p^t)=1$ 给出全部 $\varphi(p^t)$ 个 p^t 次本原单位根,均适合 (3), 这推出 $R(\xi)$ 是正规扩域. 由 (3) 也推出

$$(R(\xi)|R) \leqslant \varphi(p^t) = p^{t-1}(p-1).$$

下面我们将证明 $(R(\xi)|R) = p^{t-1}(p-1)$, 因为 ξ^k, $(k, p^t)=1$ $1 \leqslant k < p^t$ 给出 $\varphi(p^t)$ 个不同的数,故 (3) 给出

$$\Psi(x) = \prod_{\substack{(k,p^t)=1\\ 0<k<p^t}} (x-\xi^k), \tag{4}$$

在 (4) 中令 $x=1$, 我们得到

$$p = \prod_{\substack{(k,p^t)=1\\ 0<k<p^t}} (1-\xi^k), \tag{5}$$

对于任意 k, j, $(k, p) = (j, p) = 1$, 我们有

$$1 - \xi^k \equiv 0 \pmod{1 - \xi^j},$$

于是有

$$[p] = [1 - \xi]^{p^{t-1}(p-1)}. \qquad (6)$$

由 § 8 的 (8) 式知

$$(R(\xi) | R) \geqslant p^{t-1}(p - 1),$$

故

$$(R(\xi) | R) = p^{t-1}(p - 1).$$

判别式 $\triangle(1, \xi, \cdots, \xi^{\varphi(p^t)-1})$ 是形如 $\xi^i - \xi^j$ 的数的乘积，而 $p^t = \prod\limits_{i=1}^{p^t-1}(1-\xi^i)$, ξ 是一个单位数，所以 $\triangle(1, \xi, \cdots, \xi^{\varphi(p^t)-1})$ 整除 $(p^t)^l$, l 是某个正整数，故它的所有素因数皆为有理素数 p.

如果我们能够证明 $1, \xi, \cdots, \xi^{\varphi(p^t)-1}$ 是 $R(\xi)$ 的一组整底，那么定理 1 对于 $m = p^t$ 的情形便证明了，由 § 3 定理 5, $R(\xi)$ 中任一个代数整数 α 可表示为

$$\alpha = \sum_{i=0}^{\varphi(p^t)-1} \frac{x_i}{\triangle} \xi^i,$$

其中，$\triangle = \triangle(1, \xi, \cdots, \xi^{\varphi(p^t)-1})$, x_i 是有理整数，因此只需证明从

$$a_0 + a_1\xi + \cdots + a_{\varphi(p^t)-1}\xi^{\varphi(p^t)-1} \equiv 0 \pmod{p},$$

a_i 是有理整数，可以推出

$$a_i \equiv 0 \pmod{p} \quad (i = 0, 1, \cdots, \varphi(p^t) - 1).$$

由于

$$\begin{aligned}\xi^k &= (1 - (1 - \xi))^k \\ &= 1 - k(1 - \xi) + \cdots + (-1)^k(1 - \xi)^k \\ &\qquad k = 0, 1, \cdots, \varphi(p^t) - 1\end{aligned}$$

之代换行列式为 ± 1. 因此只需证明

$$b_0 + b_1(1 - \xi) + \cdots + b_{\varphi(p^t)-1}(1 - \xi)^{\varphi(p^t)-1} \equiv 0 \pmod{p}, \qquad (7)$$

推出 $p | b_i$, b_i 是有理整数 $(i = 0, 1, \cdots, \varphi(p^t) - 1)$.

由于 $p \equiv 0 \pmod{1 - \xi}$, 故 $b_0 \equiv 0 \pmod{1 - \xi}$, 由(5)即

得 $p|b_0$，在 (7) 中依次把模换成 $(1-\xi)^2, \cdots, (1-\xi)^{\varphi(p^t)}$，可依次得 $b_i \equiv 0 \pmod p$ $(i=1, \cdots, \varphi(p^t)-1)$. 这就证明了 $m=p^t$ 的情形.

现设 $m=m'p^t$，$(m', p)=1$. 由归纳法假设，对 $R(\xi_{m'})$ 定理成立. 故 $p \nmid \triangle(R(\xi_{m'}))$. 因此在 $R(\xi_{m'})$ 中，根据 Dedekind 定理有

$$[p]=P_1\cdots P_g,\quad P_1, \cdots, P_g \text{ 是不同的素理想数.} \tag{8}$$

因为 $R(\xi_{m'})$ 是正规扩域，所以 P_j 的次数为 $f(j=1, \cdots, g)$，且 $\varphi(m')=fg$. 现进一步在 $R(\xi_{m'})$ 的扩域 $R(\xi_m)$ 中分解 P_j，设 $\xi=e^{2\pi i/p^t}$ 是一个 p^t 次本原单位根，则 $\xi, \xi_{m'}$ 均在 $R(\xi_m)$ 中，故由 §7 定理 2 知在域 $R(\xi_m)$ 中有

$$(P_i, 1-\xi)^{\varphi(p^t)}=(P_i^{\varphi(p^t)}, p)=P_i,$$

于是，在 $R(\xi_m)$ 中 $[p]$ 有分解式

$$[p]=(Q_1\cdots Q_g)^{\varphi(p^t)}, \tag{9}$$

这里 $Q_i=(P_i, 1-\xi)$ $(i=1, \cdots, g)$. 由 $(p^t, m')=1$，故存在有理整数 x, y 适合 $p^tx+m'y=1$，则 $\xi_{m'}^x \cdot \xi^y=\xi_m$，因此 $R(\xi_m)=R(\xi_{m'}, \xi)$. 于是

$$\begin{aligned}(R(\xi_m)|R)&=(R(\xi_{m'}, \xi)|R(\xi_{m'}))\\ &\quad\times(R(\xi_{m'})|R)\leqslant\varphi(p^t)\varphi(m')=\varphi(m).\end{aligned}$$

设 $R(\xi_{m'})$ 的任一对代数整数 λ, μ 满足 $P_1 \nmid \mu-\lambda$，即

$$(P_1, \mu-\lambda)=[1],$$

在扩域 $R(\xi_m)$ 中有 $(Q_1^{\varphi(p^t)}, \mu-\lambda)=[1]$，故对 Q_1 的任一素因子 P，仍有 $P \nmid \mu-\lambda$，因此 Q_1 的任一素因子的次数至少是 P_1 的次数，同理 Q_i 的任一素因子的次数至少是 P_i 的次数 $(i=2, \cdots, g)$，故由 (9) 的两端取范数，可得 $(R(\xi_m)|R)\geqslant\varphi(m)$，因此得

$$(R(\xi_m)|R)=\varphi(m).$$

这也证明了 (9) 即是 $[p]$ 在 $R(\xi_m)$ 中的素理想的分解式.

因为

$$m=\prod_{i=1}^{m-1}(1-\xi_m^i),$$

所以

$$\triangle(1, \xi_m, \cdots, \xi_m^{\varphi(m)-1})$$

的每一个素因数均整除 m.

由于

$$(R(\xi_{m'}, \xi) | R(\xi)) = (R(\xi_{m'}) | R),$$

以及

$$(\triangle(1, \xi_{m'}, \cdots, \xi_{m'}^{\varphi(m')-1}), \triangle(1, \xi, \cdots, \xi^{\varphi(p^t)-1})) = 1,$$

故由引理 1, $\varphi(m)$ 个数

$$1, \cdots, \xi_{m'}^{\varphi(m')-1}, \xi, \cdots, \xi\xi_{m'}^{\varphi(m')-1}, \cdots,$$
$$\xi^{\varphi(p^t)-1}, \cdots, \xi^{\varphi(p^t)-1}\xi_{m'}^{\varphi(m')-1}$$

组成 $R(\xi_m)$ 的一组整底. 而 $\xi = \xi_m^{m'}$, $\xi_{m'} = \xi_m^{p^t}$, 故此组整底可改写成如下的形状

$$1, \xi_m^{x_1}, \cdots, \xi_m^{x_{\varphi(m)-1}},$$

因此任一整数 α 可表示为

$$\alpha = a_0 + a_1\xi_m + \cdots + a_{\varphi(m)-1}\xi_m^{\varphi(m)-1},$$

a_i 是有理整数 $(i=0, 1, \cdots, \varphi(m)-1)$, 而 $(R(\xi_m)|R)=\varphi(m)$, 故 $1, \xi_m, \cdots, \xi_m^{\varphi(m)-1}$ 是 $R(\xi_m)$ 的一组整底.

设 ξ_m 所适合的 $\varphi(m)$ 次首项系数为 1 的有理整系数不可约多项式为 $\varphi_m(x)$, 可得

$$\varphi_m(x) | x^m - 1,$$

而

$$x - 1 | \varphi_m(x)$$

或

$$x - \xi^j | \varphi_m(x), \ (j, m) > 1,$$

均不可能, 故

$$\varphi_m(x) = \prod_{\substack{j=1 \\ (j,m)=1}}^{m} (x - \xi_m^j),$$

$\varphi_m(x)$ 叫 m 阶分圆多项式. 证完.

下面给出在 $R(\xi_m)$ 中有理素数 p 分解为素理想数的乘积的两个定理.

定理 2. 设 $p \nmid m$, 且 p 模 m 的次数是 h, 则在 $R(\xi_m)$ 中 p 可

分解为 $\frac{\varphi(m)}{h}=g$ 个次数为 h 的不同的素理想数的乘积.

证. 因为 $p\nmid m$, 故 $p\nmid\triangle(R(\xi_m))$, 则在§9的(8)式中 $e=1$, 即在 $R(\xi_m)$ 中有

$$[p]=P_1\cdots P_g,$$

且 $\varphi(m)=fg$, f 是 P_j 的次数 $(1\leqslant j\leqslant g)$, 由 $(m,p)=1$,

$m=\prod_{i=1}^{m-1}(1-\xi_m^i)$, 知道 $\xi_m^i\not\equiv 1\ (\bmod P_j)(1\leqslant i\leqslant m-1)$, 否则,有某个 $i(1\leqslant i\leqslant m-1)$, 使 $\xi_m^i\equiv 1\ (\bmod P_j)$, 用共轭映射 $\sigma_l(\xi_m)=\xi_m^{(l)}$, $(l,m)=1$, 可得 $\xi_m^{li}\equiv 1\ (\bmod P_j^{(l)})$, 而 $m\nmid li$, $P_j^{(l)}$ 是 $P_1,\cdots,P_g$ 中的一个,当 l 过全部 $(l,m)=1$, $1\leqslant l<m$ 时, $P_j^{(l)}$ 过全部 $P_1,\cdots,P_g$, 这样,将有 $P_1\cdots P_g|m$, 即 $p|m$, 这与定理的条件矛盾. 此外, $\xi_m^m\equiv 1\ (\bmod P_j)$, 故 $m|p^f-1$, 推出 $f\geqslant h$.

另一方面,设 α 是一个原根模 P_j, 由定理1知

$$\alpha=a_0+a_1\xi_m+\cdots+a_{\varphi(m)-1}\xi_m^{\varphi(m)-1},$$

a_i 是有理整数 $(i=0,1,\cdots,\varphi(m)-1)$, 且

$$\alpha^{p^h}\equiv a_0+a_1\xi_m^{p^h}+\cdots+a_{\varphi(m)-1}\xi_m^{p^h(\varphi(m)-1)}\ (\bmod P_j).$$

由 $p^h\equiv 1\ (\bmod m)$, 知 $\xi_m^{p^h}=\xi_m$, 推出

$$\alpha^{p^h}\equiv\alpha\ (\bmod P_j)$$

这又得出 $h\geqslant f$, 故 $g=\frac{\varphi(m)}{h}$. 证完.

推论. 设 $p\nmid m$, 在 $R(\xi_m)$ 中, $P|[p]$, P 是素理想数, p 是有理素数. 则 $R(\xi_m)$ 的自同构 $\sigma(\xi_m)=\xi_m^p$, 保持 P 不变.

证. 可设

$$P=\{a_1\alpha_1+\cdots+a_{\varphi(m)}\alpha_{\varphi(m)},\ |a_i\in Z, i=1,\cdots,\varphi(m)\},$$

这里 $\alpha_1,\cdots,\alpha_{\varphi(m)}$ 是 P 的一组基底,用符号 $\sigma(P)$ 表示把 P 的每一个数映成它的第 p 个共轭数,则有

$$\sigma(P)=\{a_1\alpha_1^{(p)}+\cdots+a_{\varphi(m)}\alpha_{\varphi(m)}^{(p)}|a_i\in Z,\ i=1,\cdots,\varphi(m)\}=P^{(j)}.$$

设 $\alpha_i=g_i(\xi_m)$, $i=1,\cdots,\varphi(m)$, $g_i(x)$ 是次数不超过

$\varphi(m)-1$ 次的整系数多项式，而

$$\alpha_i^{(p)}=g_i(\xi_m^p)\equiv g_i^p(\xi_m)\ (\bmod p),$$

由于 $p\in P$，故 $\alpha_i^{(p)}=g_i^p(\xi_m)+p\lambda\in P$，$(i=1,\cdots,\varphi(m))$，这里 λ 是 $R(\xi_m)$ 中的一个代数整数．于是有 $P^{(p)}\subseteq P$，即 $P|P^{(p)}$．另一方面，$p\nmid m$，$P^{(p)}$ 是 P 的共轭理想数，而 $[p]=P_1\cdots P_g$，故 $P^{(p)}$ 是 $P_1,\cdots,P_g$ 中的某一个，即是一个素理想数，于是有 $\sigma(P)=P^{(p)}=P$，这就证明自同构 $\sigma(\xi_m)=\xi_m^p$ 保持 P 不变．证完．

定理 3．设 $m=p^tm_1$，$(p,m_1)=1$，p 模 m_1 的次数是 h，则在 $R(\xi_m)$ 中有

$$[p]=(Q_1\cdots Q_g)^{\varphi(p^t)},\quad g=\frac{\varphi(m_1)}{h},$$

这里 Q_i 是次数为 h 的素理想数（$i=1,\cdots,g$）．

证．由定理 2 知在 $R(\xi_{m_1})$ 中

$$[p]=P_1\cdots P_g,\qquad g=\frac{\varphi(m_1)}{h},$$

而在 $R(\xi_m)$ 中，由 (9) 式得

$$[p]=(Q_1\cdots Q_g)^{\varphi(p^t)}.$$

设 Q_i 的次数为 f，则由上式得

$$\varphi(m)=\varphi(p^t)fg=\varphi(p^t)f\,\frac{\varphi(m_1)}{h},$$

故 $f=h$．证完．

第六章　二次域和分圆域内的DFT构造

本章着重讨论用二次域 $R(\sqrt{m})$ 和分圆域 $R(\eta)$ 的整数剩余类环来计算域中整数序列的卷积问题，数论变换的有关理论得到了推广，在这些域里，具有循环卷积性质的变换的构造和个数等问题，都得到了解决.

§1. 计算复整数序列的卷积

当 M 取 Mersenne 素数时的数论变换叫做 Mersenne 数变换，由于此时 $O(M)=O(2^p-1)=2^p-2=2(2^{p-1}-1)$，它能卷积的序列长度 N 的标准分解式中 2 的方幂最高是 1，故不能作快速演段，因而我们没有讨论这类数论变换.

如果对全体复整数 $a+bi$，$a,b\in Z$（即 $R(i)$ 中的整数），用模 q 分类（q 取 Mersenne 素数），在所得剩余类间定义适当的加法和乘法运算，可得一个有 q^2 个元素的有限域，记为 $GF(q^2)$，在此有限域中，可计算复整数序列的卷积，其序列长度N的标准分解式中所含 2 的方幂可大为提高．这是 Mersenne 数变换的一个推广，当 $N=2^m$ 时，同样可类似 FFT 作快速演段．本节将着重讨论这一类变换.

1. 复数论变换

先用复整数分类的办法，来构造一个 $GF(q^2)$，这里 $q=2^p-1$ 是一个 Mersenne 素数．把全体复整数 $a+bi$ 用模 q 分类．即当且仅当 $\alpha\equiv\beta(\bmod q)$ 时，α,β 属同一类，这里 α、β 为任给的两个复整数，即 $R(i)$ 的代数整数．于是，我们得到一个剩余类，设其剩余系（即每类中取一个代表）为

$$F=\{a+bi\,|\,a,b\in GF(q)\},$$

在F中定义加法

$$(a+bi)+(c+di)=\langle a+c\rangle_q+\langle b+d\rangle_q i,$$

以及乘法

$$(a+bi)\cdot(c+di)=\langle ac-bd\rangle_q+\langle ad+bc\rangle_q i,$$

则由$\left(\frac{-1}{q}\right)=-1$，知$F$成域，其元素个数为$q^2$，故可记

$$GF(q^2)=\{a+bi\,|\,a,b\in GF(q)\}.$$

设$x_0,x_1,\cdots,x_{N-1}\in GF(q^2)$，可类似地定义$GF(q^2)$上的DFT如下：

如果作用在序列$x_0,x_1,\cdots,x_{N-1}$上的一个变换

$$X_k=\sum_{n=0}^{N-1}x_n\alpha^{nk}\quad(k=0,1,\cdots,N-1)\quad \alpha\in GF(q^2),$$

有如下形状的逆变换

$$x_n=N^{-1}\sum_{k=0}^{N-1}X_k\alpha^{-nk}\qquad(n=0,1,\cdots,N-1),$$

且具有循环卷积性质，则称此变换为$GF(q^2)$上长为N的一个DFT，或复数论变换. 用与第三章§2定理1类似的证法可证下面的定理.

定理. $GF(q^2)$上长为N的一个复数论变换存在的充分必要条件是α是$GF(q^2)$中的N次本原单位根.

推论1. $GF(q^2)$上长为N的复数论变换存在的充分必要条件是$N|q^2-1$.

推论2. 设$N|q^2-1$，则$GF(q^2)$上共有$\varphi(N)$个长为N的复数论变换.

以上关于$GF(q^2)$上DFT的定义和结果，在任意有限域$GF(p^n)$上可类似地定义和证明.

因为$q=2^p-1$，故由$N|q^2-1=2^{p+1}(2^{p-1}-1)$知，$N$的标准分解式中2的方幂最高可达$p+1$. 所以，复数论变换可快速卷积的序列之最大长度为$2^{p+1}$. 对于长度是2的方幂的复数论变换，可用类似FFT的快速演段来计算，叫做快速复数论变换.

2. $GF(q^2)$ 中 $N(N=2^k, 1\leqslant k\leqslant p+1)$ 次本原单位根的计算

由上一小节的定理 1 我们知道，求出 $GF(q^2)$ 上的一个N次本原单位根，也就构造出了一个 $GF(q^2)$ 上的长为N的一个 DFT.

性质 1. α 是N次本原单位根的充分必要条件是

$$\alpha^{\frac{N}{2}}\equiv -1 \pmod q.$$

证. 如果 $\alpha^N\equiv 1 \pmod q$，则有

$$(\alpha^{\frac{N}{2}}+1)(\alpha^{\frac{N}{2}}-1)\equiv 0 \pmod q,$$

而由 $\left(\frac{-1}{q}\right)=-1$ 知 q 是 $R(i)$ 中的素数，且 $R(i)$ 中整数的唯一分解定理成立，故由 α 是N次本原单位根可得 $\alpha^{\frac{N}{2}}\equiv -1 \pmod q$（用有限域的性质也易证明）.

反之，若 $\alpha^{\frac{N}{2}}\equiv -1 \pmod q$，则 $\alpha^N\equiv 1 \pmod q$，如果 α 是 l 次本原单位根，$l<N$，$l|N$，可推出 $l\left|\frac{N}{2}\right.$，从而得到矛盾结果 $\alpha^{\frac{N}{2}}\equiv 1 \pmod q$，故必有 $l=N$.

性质 2. $(a+bi)^{2^p}\equiv a^2+b^2 \pmod q$.

证.

$$(a+bi)^{2^p}=(a+bi)^{2^p-1}(a+bi)\equiv(a-bi)(a+bi)$$
$$=a^2+b^2 \pmod q.$$

由此可立即推出下面一个性质.

性质 3. $\alpha=a+bi$ 是一个 2^{p+1} 次本原单位根的充分必要条件是 $a^2+b^2\equiv -1 \pmod q$.

性质 4. $2^{2^{p-2}}+(-3)^{2^{p-2}}i$ 是 $GF(q^2)$ 中的一个 2^{p+1} 次本原单位根.

证. 因 $\left(\frac{2}{q}\right)=1$，$\left(\frac{-3}{q}\right)=1$，$q=2^p-1$，

故

$$2^{2^{p-1}}\equiv 2 \pmod q,\qquad (-3)^{2^{p-1}}\equiv -3 \pmod q,$$

符合性质 3 给出的条件，故是一个 2^{p+1} 次本原单位根.

性质 5.

$$[2^{2^{p-2}}+(-3)^{2^{p-2}}]^l \qquad (l=1,3,\cdots,2^{p+1}-1),$$

给出 $GF(q^2)$ 中全部 2^{p+1} 次本原单位根.

证. 由性质 1 知,它们都是 2^{p+1} 次本原单位根,且两两模 q 不同余,而 $\varphi(2^{p+1})=2^p$, 故可知给出了全部 2^{p+1} 次本原单位根.

性质 6. 设 $N=2^k$, $1\leqslant k\leqslant p+1$, 则

$$[2^{2^{p-2}}+(-3)^{2^{p-2}}i]^{2^{p+1-k}l} \qquad (l=1,3,\cdots,2^k-1),$$

给出了 $GF(q^2)$ 中全部 2^k 次本原单位根.

证. 可完全仿照性质 5 来证明.

可用 $2p$ 位字长的硬件进行复整数 $a+bi$ 模 q 的乘、加法运算. 为了使乘 2 的方幂运算简单,显然是把 N 次 ($N=2^k$, $1\leqslant k\leqslant p+1$) 本原单位根 α 的实部 a 和虚部 b 用二进制表示,且位数越少越好.

例. $q=2^5-1=31$, $2^{p+1}=2^6=64$, 求出全部 $GF(31^2)$ 中的全部 8 次本原单位根.

由于

$$a=2^8\equiv 8\ (\mathrm{mod}\ 31), \qquad b=(-3)^8\equiv 20\ (\mathrm{mod}\ 31),$$

故 $\alpha=8+20i$ 是 $GF(31^2)$ 中的一个 64 次本原单位根. 所以由性质 6 知 $(8+20i)^{8l}$, $l=1,3,5,7$ 给出了全部 8 次本原单位根,计算结果是 $27+4i$, $4+4i$, $4+27i$, $27+27i$, 其中 $4+4i$ 构成的复数论变换,计算时最为方便.

3. 另一个算法

对于不太大的 q, 不用上一小节的方法,而用查平方表和分类的算法来计算全部 2^{p+1} 次本原单位根,要简便一些.

由上一小节的性质 3 知求出 $GF(q^2)$ 上的全部 2^{p+1} 次本原单位根只需求出同余式

$$a^2+b^2\equiv -1\ (\mathrm{mod}\ q) \qquad (0\leqslant a<q,\ 0\leqslant b<q) \tag{1}$$

的全部解 (a,b), 其解的个数必为 $\varphi(2^{p+1})=2^p$ 个.

由 $\left(\dfrac{-1}{q}\right)=-1$ 知 $a\neq 0$, $b\neq 0$. 还有(1)中 $a\neq b$, 否

则，由 $a=b$，从(1)可推出 $2a^2\equiv -1 \pmod q$，即 $(2a)^2\equiv -2 \pmod q$，这与 $\left(\frac{-2}{q}\right)=\left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)=-1$ 矛盾。

这样，如果

$$(a,b)\qquad \left(0<a<b\leqslant \frac{q-1}{2}\right) \tag{2}$$

是(1)的一组解，则由(2)可给出(1)的另7组解

$$(q-a,b),\quad (q-a,q-b),\quad (a,q-b),$$
$$(b,a),\quad (q-b,a),\quad (b,q-a),\quad (q-b,q-a), \tag{3}$$

如把(2)和由(2)变出的(3)定义成一类，则(1)的全部解 (a,b) 将分成 2^{p-3} 个类。知道了一类中的任何一个解，均可由(2)得出(3)的方法得出类中的其余7个解，故均可定义为类的代表，我们把(2)叫做一个类的标准代表。只要求出了各类的代表，全部解即可求得。

利用平方表，下面列出 $q=2^7-1$ 时，$GF(q^2)$ 的全部 2^8 次本原单位根16个类的标准代表

(2, 54), (3, 25), (8, 58), (10, 36), (13, 46),
(16, 39), (19, 20), (27, 26), (28, 55), (29, 38),
(30, 49), (34, 42), (35, 60), (40, 47), (56, 61),
(57, 59).

4. 用 $GF(q^2)$ 上的复数论变换计算复整数的卷积

设 $x_n=a_n+b_ni$，$h_n=c_n+d_ni$，均为 $Z(i)$ 中的整数，$(n=0,1,\cdots,N-1)$，其循环卷积为

$$\begin{aligned}y_n&=\sum_{k=0}^{N-1}x_kh_{\langle n-k\rangle_N}\\&=\sum_{k=0}^{N-1}(a_k+b_ki)(c_{\langle n-k\rangle_N}+d_{\langle n-k\rangle_N}i)\\&=\sum_{k=0}^{N-1}(a_kc_{\langle n-k\rangle_N}-b_kd_{\langle n-k\rangle_N})\end{aligned}$$

$$+\sum_{k=0}^{N-1}(b_k c_{\langle n-k\rangle_N}+a_k d_{\langle n-k\rangle_N})i. \tag{4}$$

用 $GF(q^2)$ 上的复数论变换计算 (4) 式，得到

$$y_n \equiv u_n + v_n i \pmod q, \quad u_n, v_n \in GF(q)$$

$(n=0,1,\cdots,N-1)$，如果选择 q 对 $(n=0,1,\cdots,N-1)$ 均有

$$\left|\sum_{k=0}^{N-1}(a_k c_{\langle n-k\rangle_N}-b_k d_{\langle n-k\rangle_N})\right|$$
$$\leqslant \sum_{k=0}^{N-1}(|a_k||c_{\langle n-k\rangle_N}|+|b_k||d_{\langle n-k\rangle_N}|)<\frac{q}{2} \tag{5}$$

和

$$\left|\sum_{k=0}^{N-1}(b_k c_{\langle n-k\rangle_N}+a_k d_{\langle n-k\rangle})\right|$$
$$\leqslant \sum_{k=0}^{N-1}(|b_k||c_{\langle n-k\rangle_N}|+|a_k||d_{\langle n-k\rangle_N}|)<\frac{q}{2}, \tag{6}$$

则取 u_n，v_n 模 q 的绝对最小剩余，即可求出 (4)．设 M^2 个元素的环 $R_{M^2}=\{a+bi \mid a, b\in Z_M\}$，这里 $M=q_1\cdots q_s$，q_i 是不同的 Mersenne 素数，由孙子定理以及直和

$$S_{M^2}=GF(q_1^2)\dotplus\cdots\dotplus GF(q_s^2)=\{(\alpha_1,\cdots,\alpha_s)\mid \alpha_i\in GF(q_i^2),$$
$$i=1,\cdots,s\}$$

与 R_{M^2} 同构，可以减少用 R_{M^2} 上的复数论变换求复整数的卷积时所需的机器字长．下一节，我们将讨论更一般的情形．

§2. 在二次域 $R(\sqrt{m})$ 里计算卷积

在这节里，我们将通过二次域 $R(\sqrt{m})$ 的全体代数整数模 M 的剩余类环上的 DFT，来计算代数整数的卷积，与 Z_M 上的 DFT 一样，我们将给出存在这样的 DFT 的充分必要条件、它们的算法和全部个数．

在给出主要定理之前，先证明几个性质.

性质 1. 设 $M > 1$; M 是奇数,

$$I_{M^2}(\theta) = \{a + b\theta \mid a, b \in Z_M\}, \tag{1}$$

其中 θ 等于

$$\theta = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod 4, \\ \dfrac{\sqrt{m}+1}{2}, & m \equiv 1 \pmod 4), \end{cases} \tag{2}$$

即 1, θ 是二次域 $R(\sqrt{m})$ 的一组整底, m 是无平方因子的整数. 我们在 (1) 中定义加法

$$(a + b\theta) + (c + d\theta) = \langle a + c\rangle_M + \langle c + d\rangle_M\theta, \tag{3}$$

和乘法

$$(a+b\theta)(c+d\theta) = \begin{cases} \langle ac + bdm\rangle_M + \langle ad + bc\rangle_M\theta, \\ \qquad m \equiv 2, 3 \pmod 4, \\ \left\langle ac + bd\dfrac{m-1}{4}\right\rangle_M + \langle ad + bc + bd\rangle_M\theta, \\ \qquad m \equiv 1 \pmod 4, \end{cases} \tag{4}$$

则对运算 (3) 和 (4), $I_{M^2}(\theta)$ 构成一个有单位元素的、元素个数是 M^2 的可换环. 如果 $M = q$ 是一个奇素数, $\left(\dfrac{m}{q}\right) = -1$, 则环 $I_{q^2}(\theta)$ 构成一个域, 记为 $GF(q^2)$.

证. 由环的定义和性质 $\langle x + y\rangle_l = \langle\langle x\rangle_l + \langle y\rangle_l\rangle_l$, $\langle xy\rangle_l = \langle\langle x\rangle_l\langle y\rangle_l\rangle_l$, $l' \mid l$, $\langle\langle x\rangle_l\rangle_{l'} = \langle x\rangle_{l'}$, 可直接验证成环, 这里 l 和 l' 均为正整数. 现设 $M = q$, $\left(\dfrac{m}{q}\right) = -1$, $\alpha \in I_{q^2}(\theta)$, $\alpha = a + b\theta \neq 0$, α 的范数 $N(\alpha)$ 适合

$$\begin{aligned} N(\alpha) &= \alpha\bar{\alpha} = (a + b\theta)(a + b\bar{\theta}) \\ &= \begin{cases} a^2 - b^2 m, & m \equiv 2, 3 \pmod 4, \\ a^2 + ab + b^2\dfrac{1-m}{4}, & m \equiv 1 \pmod 4, \end{cases} \end{aligned} \tag{5}$$

由 q 是素数知 $(q, N(\alpha)) = 1$ 或者 $q \mid N(\alpha)$. 因为 $q \nmid \alpha$, $\left(\dfrac{m}{q}\right) =$

-1，故在 $m\equiv 2, 3 \pmod 4$ 时，易知 $q\nmid N(\alpha)$，而在 $m\equiv 1 \pmod 4$ 时，由(5)给出 $4N(\alpha)=(2a+b)^2-b^2m$，仍有 $q\nmid N(\alpha)$。总之，得出 $(q, N(\alpha))=1$，设 $N(\alpha)u\equiv 1 \pmod q$，$0<u<q$，则 $\alpha^{-1}=u\bar{\alpha}$，这里 $\bar{\alpha}$ 表示 α 的共轭数，这就证明 $I_{q^2}(\theta)$ 的任一非零元素有逆元素，即知 $I_{q^2}(\theta)$ 成域.

性质1给出的环 $I_{M^2}(\theta)$ 与二次域 $R(\sqrt{m})$里的整数对理想数 $[M]$ 分类所组成的模 $[M]$ 剩余类环同构，因而就把 $I_{M^2}(\theta)$ 叫做 $R(\sqrt{m})$ 的代数整数模M的剩余类环.

性质 2. 设 $M>1$，M 是奇数，$M=m_1\cdots m_r$，$(m_i, m_j)=1$ $(1\leqslant i<j\leqslant r)$，定义环 $I_{m_j^2}(\theta)(j=1,\cdots,r)$ 的直和是

$$\begin{aligned}S_{M^2}(\theta)&=I_{m_1^2}(\theta)\dotplus\cdots\dotplus I_{m_r^2}(\theta)\\&=\{(\alpha_1,\cdots,\alpha_r)\,|\,\alpha_j\in I_{m_j^2}(\theta)(j=1,\cdots,r)\}\end{aligned}$$

在 $S_{M^2}(\theta)$ 中定义加法

$$(\alpha_1,\cdots,\alpha_r)+(\beta_1,\cdots,\beta_r)=(\alpha_1+\beta_1,\cdots,\alpha_r+\beta_r), \quad (6)$$

和乘法

$$(\alpha_1,\cdots,\alpha_r)(\beta_1,\cdots,\beta_r)=(\alpha_1\beta_1,\cdots,\alpha_r\beta_r), \quad (7)$$

则 $S_{M^2}(\theta)$ 对于运算 (6) 和 (7) 构成一个有单位元素的、元素个数是 M^2 的可换环，且与环 $I_{M^2}(\theta)$ 同构.

证. 定义 $I_{M^2}(\theta)$ 到 $S_{M^2}(\theta)$ 上的一个映射 σ:

$$\sigma(a+b\theta)=(\langle a\rangle_{m_1}+\langle b\rangle_{m_1}\theta,\cdots,\langle a\rangle_{m_r}+\langle b\rangle_{m_r}\theta), \quad (8)$$

容易验算

$$\begin{aligned}\sigma((a+b\theta)+(c+d\theta))&=\sigma(a+b\theta)+\sigma(c+d\theta),\\ \sigma((a+b\theta)(c+d\theta))&=\sigma(a+b\theta)\sigma(c+d\theta).\end{aligned}$$

再设

$$\sigma^{-1}(0,\cdots,0)=a+b\theta,$$

由$a\equiv 0 \pmod{m_j}$，$b\equiv 0 \pmod{m_j}$ $(j=1,\cdots,r)$ 和孙子定理知在 Z_M 上有唯一解 $a=b=0$，故 σ 是一个同构映射，即得 $I_{M^2}(\theta)\simeq S_{M^2}(\theta)$，$S_{M^2}(\theta)$ 对于运算 (6) 和 (7) 构成一个有单位元素的、元素个数是 M^2 的可换环.

这里需要指出，性质 2 中的直和以及同构，显然都与 $M = m_1 \cdots m_r$，$(m_i, m_j) = 1$ $(1 \leqslant i < j \leqslant r)$ 有关，为方便起见，我们都采用了相同的符号；同样，$R(\sqrt{m})$、$I_{M^2}(\theta)$、$S_{M^2}(\theta)$ 中的乘、加法运算分别都是不同的，我们也都采用了相同的符号.

性质 3. 设 p 是奇素数，$\left(\frac{m}{p}\right) = -1$，$a_i$ 是 $R(\sqrt{m})$ 的整数 $(i = 0, 1, \cdots, n)$，同余式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \pmod{p}$$

在 $R(\sqrt{m})$ 上的整数解的个数 $\leqslant n$，重解计算在内，与有理整数一样，这里解的个数是指非同余的解的个数.

证. 由于 $\left(\frac{m}{p}\right) = -1$，故 $[p]$ 是素理想数，再由理想数的唯一分解定理，与第一章 2.8 小节的定理类似可证.

性质 4. 设 p 是奇素数，$\left(\frac{m}{p}\right) = -1$，$a_i$ $(i = 0, 1, \cdots, n)$ 是 $R(\sqrt{m})$ 的整数，同余式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p^l}$$

当 $f(x) \equiv 0 \pmod{p}$ 与 $f'(x) \equiv 0 \pmod{p}$ 无公解，则

$$f(x) \equiv 0 \pmod{p^l}$$

解的个数等于

$$f(x) \equiv 0 \pmod{p}$$

解的个数. 以上同余式的解指 $R(\sqrt{m})$ 里的整数.

证. 用归纳法证明. $l = 1$，自不必证. 设 $l \geqslant 2$，整数 $x_1 = a + b\theta$ 是 $f(x) \equiv 0 \pmod{p^{l-1}}$ 的一个解，可设 $0 \leqslant a < p^{l-1}$，$0 \leqslant b < p^{l-1}$，则

$$f(x_1 + p^{l-1}y) \equiv f(x_1) + p^{l-1}yf'(x_1) \pmod{p^l}, \tag{9}$$

而 $p \nmid f'(x_1)$，$\left(\frac{m}{p}\right) = -1$，由性质 1 知，$\frac{f(x_1)}{p^{l-1}} + yf'(x_1) \equiv 0 \pmod{p}$ 有唯一的 y 模 p，使 $x_1 + p^{l-1}y$ 是 $f(x) \equiv 0 \pmod{p^l}$ 的解，这里，显然，$f(x) \equiv 0 \pmod{p^{l-1}}$ 不同的解给出 $f(x) \equiv 0 \pmod{p^l}$ 不同的解.

反之，任给 $\xi = u + v\theta$ 是 $f(x) \equiv 0 \pmod{p^l}$ 的一个解，显然 ξ 可表示为 $\xi = p^{l-1}s + \xi_1$，这里 s 是 $R(\sqrt{m})$ 的整数，$\xi_1 = \langle u \rangle_{p^{l-1}} + \langle v \rangle_{p^{l-1}}\theta$ 是 $f(x) \equiv 0 \pmod{p^{l-1}}$ 的一个解，s 是唯一的。如果 $\xi' = u' + v'\theta$ 是 $f(x) \equiv 0 \pmod{p^l}$ 的另一个解，则 $\xi \not\equiv \xi' \pmod{p^l}$，而 ξ' 可表示为 $\xi' = p^{l-1}s' + \xi_1'$，这里 s' 是唯一的，$\xi_1' = \langle u' \rangle_{p^{l-1}} + \langle v' \rangle_{p^{l-1}}\theta$ 是 $f(x) \equiv 0 \pmod{p^{l-1}}$ 的一个解，则有 $\xi_1 \not\equiv \xi_1' \pmod{p^{l-1}}$，反之 $\xi_1 = \xi_1'$，可由 (9) 知 $s \equiv s' \pmod{p}$，从而推出 $\xi - \xi' = p^{l-1}(s - s') \equiv 0 \pmod{p^l}$，得到矛盾结果。这就证明了在性质 4 的条件下，$f(x) \equiv 0 \pmod{p^l}$ 和 $f(x) \equiv 0 \pmod{p^{l-1}}$ 解的个数相等，从而完成了归纳法证明。

现在我们引入环 $I_{M^2}(\theta)$ 上序列的循环卷积和长为 N 的 DFT 的定义。

设序列 x_i、h_i $(i = 0, 1, \cdots, N-1) \in I_{M^2}(\theta)$，它们的循环卷积是指

$$y_n = \sum_{k=0}^{N-1} x_k h_{\langle n-k \rangle_N} \quad (n = 0, 1, \cdots, N-1).$$

设变换

$$X_k = \sum_{n=0}^{N-1} x_n \alpha^{nk} \quad (k = 0, 1, \cdots, N-1), \quad \alpha \in I_{M^2}(\theta) \quad (10)$$

有逆变换[1)]

$$x_n = N^{-1} \sum_{k=0} X_k \alpha^{-nk} \quad (n = 0, 1, \cdots, N-1),$$

并有循环卷积性质

$$X_k \cdot H_k = Y_k (k = 0, 1, \cdots, N-1),$$

则称 (10) 给出的变换是 $I_{M^2}(\theta)$ 上的一个长为 N 的 DFT，这里

$$H_k = \sum_{n=0}^{N-1} h_n \alpha^{nk},$$

$$Y_k = \sum_{n=0}^{N-1} y_n \alpha^{nk} \quad (k = 0, 1, \cdots, N-1).$$

---

1) 可以证明，逆变换的形状可由定义的其余条件推出。

用第三章§2定理1的证明方法可得下面的定理.

定理1. (10)是环 $I_{M^2}(\theta)$ 上的一个长为 N 的 DFT 的充分必要条件是 $(N, M)=1$, 且

$$\sum_{j=0}^{N-1}(\alpha^u)^j=0 \quad (u=1,\cdots,N-1).$$

下面我们将给出几个构造性的结果.

定理2. 设 $M=q_1^{l_1}\cdots q_r^{l_r}$, $q_i(i=1,\cdots,r)$ 是不同的奇素数,且满足 $\left(\frac{m}{q_i}\right)=-1 \quad (i=1,\cdots,r)$, 则(10)是环 $I_{M^2}(\theta)$ 上长为 N 的 DFT 的充分必要条件是 $(N, M)=1$, α_i 是环 $I_{q_i^{2l_i}}(\theta)$ 的 N 次单位根,且 α_i 是 $GF(q_i^2)$ 的 N 次本原单位根 $(i=1,\cdots,r)$, 这里 $\sigma(\alpha)=(\alpha_1,\cdots,\alpha_r)\in S_{M^2}(\alpha)$, σ 是由(8)给出的同构映射.

证. 设(10)给出的变换是 $I_{M^2}(\theta)$ 上的 DFT, 则 $(N, M)=1$,

$$\sum_{j=0}^{N-1}(\alpha^u)^j=0 \qquad (u=1,\cdots,N-1),$$

故

$$\sum_{j=0}^{N-1}(\alpha_i^u)^j\equiv 0 \pmod{q_i^{l_i}} \ (i=1,\cdots,r, u=1,\cdots,N-1),$$

于是

$$\alpha_i^N-1=(\alpha_i-1)\sum_{j=0}^{N-1}\alpha_i^j\equiv 0 \pmod{q_i^{l_i}},$$

即 α_i 是 $I_{q_i^{2l_i}}(\theta)$ 的 N 次单位根 $(i=1,\cdots,r)$. 又如存在某对 $1\leqslant u\leqslant N-1$, $1\leqslant i\leqslant r$, 使 $q_i|\alpha_i^u-1$, 则由

$$\sum_{j=0}^{N-1}(\alpha_i^u)^j\equiv 0 \pmod{q_i}$$

可得 $q_i|N$, 与 $(N, M)=1$ 矛盾. 必要性已经证明.

现证充分性. 由 $R(\sqrt{m})$ 的基数 $\triangle=4m$ 或 m, $\left(\frac{m}{q_i}\right)=-1$ $(i=1,\cdots,r)$, 故 $[q_i]$ $(i=1,\cdots,r)$ 是素理想,而

$$(\alpha_i^u - 1)\sum_{j=0}^{N-1}(\alpha_i^u)^j = (\alpha_i^u)^N - 1 \equiv 0 \pmod{[q_i]^{l_i}}$$

$$(i = 1, \cdots, r, u = 1, \cdots, N-1)$$

而

$$[q_i] \nmid \alpha_i^u - 1 (i = 1, \cdots, r, u = 1, \cdots, N-1),$$

由理想数的唯一分解定理可得

$$\sum_{j=0}^{N-1}(\alpha_i^u)^j \equiv 0 \pmod{q_i^{l_i}} \quad (i = 1, \cdots, r),$$

再由同构映射得

$$\begin{aligned} 0 &= \sigma^{-1}(0, 0, \cdots, 0) \\ &= \sigma^{-1}\left(\sum_{j=0}^{N-1}(\alpha_1^u)^j, \cdots, \sum_{j=0}^{N-1}(\alpha_r^u)^j\right) \\ &= \sum_{j=0}^{N-1}(\alpha^u)^j \quad (u = 1, \cdots, N-1), \end{aligned}$$

而 $(N, M) = 1$，故由定理 1 知，(10) 给出 $I_{M^2}(\theta)$ 上一个长为 N 的 DFT。

定理 3. 设 $M = q_1^{l_1} \cdots q_r^{l_r}$，$q_i$ 是不同的奇素数，$\left(\frac{m}{q_i}\right) = -1$ $(i = 1, \cdots, r)$，存在 $I_{M^2}(\theta)$ 上长为 N 的 DFT 的充分必要条件是 $N|(q_1^2 - 1, \cdots, q_r^2 - 1)$。

证．由定理 2 立即可得必要性 $N|(q_1^2 - 1, \cdots, q_r^2 - 1)$．现设 $N|(q_1^2 - 1, \cdots, q_r^2 - 1)$，故 $(N, M) = 1$，且存在 $GF(q_i^2)$ 的 N 次本原单位根 $\beta_i (i = 1, \cdots, r)$，再设 $\alpha_i = \beta_i^{q_i^{2(l_i-1)}}$ $(i = 1, \cdots, r)$，用第三章 §2 的算法二类似可证 $\alpha_i^N \equiv 1 \pmod{q_i^{l_i}}$ $(i = 1, \cdots, r)$，且易知 $\alpha_i \equiv \beta_i \pmod{q_i}$ $(i = 1, \cdots, r)$，这就证明了 $\alpha = \sigma^{-1}(\alpha_1, \cdots, \alpha_r)$ 合定理 2 的条件，故存在 $I_{M^2}(\theta)$ 上长为 N 的 DFT。

定理 4. 设 $M = q_1^{l_1} \cdots q_r^{l_r}$，$q_i$ 是不同的奇素数，$\left(\frac{m}{q_i}\right) = -1$ $(i = 1, \cdots, r)$，$N|(q_1^2 - 1, \cdots, q_r^2 - 1)$，则 $I_{M^2}(\theta)$ 上长为 N

的 DFT 有 $\varphi^r(N)$ 个.

证. 由于 $N|(q_1^2-1,\cdots,q_r^2-1)$, 则 $GF(q_i^2)$ 中恰有 $\varphi(N)$ 个 N 次本原单位根 $\beta_{1,i},\cdots,\beta_{\varphi(N),i}$, 则得出 $\alpha_{1,i}=\beta_{1,i}^{q_i^{2(l_i-1)}},\cdots,\alpha_{\varphi(N),i}=\beta_{\varphi(N),i}^{q_i^{2(l_i-1)}}$ 共 $\varphi(N)$ 个 $I_{q_i^{2l_i}}(\theta)$ 的N次单位根,而对 $1\leqslant j_1<j_2\leqslant\varphi(N)$, $\alpha_{j_1,i}\not\equiv\alpha_{j_2,i}\pmod{q_i^{l_i}}$, 否则推出 $\beta_{j_1,i}\equiv\beta_{j_2,i}\pmod{q_i}$, 这将得到一个矛盾结果. 于是 $GF(q_1^2)\dotplus\cdots\dotplus GF(q_r^2)$ 的 $\varphi^r(N)$ 个不同的元素

$$(\beta_{j_1,1},\beta_{j_2,2},\cdots,\beta_{j_r,r}),\ 1\leqslant j_t\leqslant\varphi(N)\quad(t=1,\cdots,r),\tag{11}$$

产生 $S_{M^2}(\theta)=I_{q_1^{2l_1}}(\theta)\dotplus\cdots+I_{q_r^{2l_r}}(\theta)$ 的 $\varphi^r(N)$ 个不同的元素

$$(\alpha_{j_1,1},\alpha_{j_2,2},\cdots,\alpha_{j_r,r}),\ 1\leqslant j_t\leqslant\varphi(N)\quad(t=1,\cdots,r),\tag{12}$$

故由同构映射 $\sigma^{-1}(\alpha_{j_1,1},\cdots,\alpha_{j_r,r})=\alpha$ 得出 $I_{M^2}(\theta)$ 中 $\varphi^r(N)$ 个不同的 α, 即 $I_{M^2}(\theta)$ 上长为N的 DFT 的个数 $T\geqslant\varphi^r(N)$.

现任给一个长为N的 DFT, 由定理 2, 即给出一个 $\alpha\in I_{M^2}(\theta)$, $\sigma(\alpha)=(\alpha_1,\cdots,\alpha_r)$, α_i 是 $I_{q_i^{2l_i}(\theta)}$ 的N次单位根, 且是 $GF(q_i^2)$ 的N次本原单位根,故此 α 对应(11)中的一个元素,现设 α, α' (此处 $\sigma(\alpha')=(\alpha_1',\cdots,\alpha_r')$ 给出 $I_{M^2}(\theta)$ 上一个长为N的 DFT)对应 (11) 中同一个元素 $(\beta_{j_1^0,1},\cdots,\beta_{j_r^0,r})$, 而 α_i, α_i' 均适合

$$x^N\equiv 1\pmod{q_i^{l_i}}\quad(i=1,\cdots,r),\tag{13}$$

易知 α_i, α_i' 均为 $I_{q_i^{2l_i}}(\theta)$ 的N次本原单位根,故 $\alpha_i,\alpha_i^2,\cdots,\alpha_i^N$ 是 (13) 的N个不同的解,由性质 3 和性质 4 知, 它们是 (13) 的全部解,于是

$$\alpha_i'\equiv\alpha_i^{t_i}\pmod{q_i^{l_i}}\quad(i=1,\cdots,r)\quad(1\leqslant t_i\leqslant N),$$

但 $\alpha_i'\equiv\alpha_i\equiv\beta_{j_i^0,i}\pmod{q_i}$,故有

$$\beta_{j_i^0,i}\equiv\beta_{j_i^0,i}^{t_i}\pmod{q_i},$$

而 $\left(\dfrac{m}{q_i}\right)=-1$, 上式推出 $\beta_{j_i^0,i}^{t_i-1}\equiv 1\pmod{q_i}$, $N|t_i-1$, 即得 $t_i=1$, 于是 $\alpha_i'=\alpha_i(i=1,\cdots,r)$, 便有 $\alpha=\alpha'$, 故 $T\leqslant\varphi^r(N)$, 这就证明了 $T=\varphi^r(N)$.

定理 5. 设

$$M=\prod_{i=1}^{r}F_{n_i}\quad(n_1<\cdots<n_r),$$

$$F_{n_i}=2^{2^{n_i}}+1=\prod_{k=1}^{s_i}q_{k,i}^{l_{k,i}},$$

$l_{k,i}\geqslant 1$, $q_{k,i}$ 是不同的素数，满足$\left(\frac{m}{q_{k,i}}\right)=-1$ $(k=1,\cdots,s_i,$ $i=1,\cdots,r)$，则环 $I_{M^2}(\theta)$ 上存在长为 2^{n_1+3} 的 DFT. 当用长为 2^{n_1+3} 的 DFT 计算 $I_{M^2}(\theta)$ 上序列的卷积时，可通过在环 $I_{F^2_{n_i}}(\theta)$ 上 $(i=1,\cdots,r)$ 分别求出序列的卷积，再由同构 σ^{-1} 求出.

证. 因为 F_n 的每一个素因子形如 $k2^{n+2}+1\ (k>0)$，以及定理 3，即知存在 $I_{M^2}(\theta)$ 上长为 2^{n_1+3} 的 DFT，再由定理 1 知存在 (10) 中的 α 满足

$$\sum_{j=0}^{2^{n_1+3}-1}(\alpha^u)^j\equiv 0\ (\mathrm{mod}\ M)\quad(u=1,\cdots,2^{n_1+3}-1),$$

而

$$(F_{n_i},F_{n_j})=1\quad(1\leqslant i<j\leqslant r),$$

由性质 2 知

$$I_{M^2}(\theta)\simeq S_{M^2}(\theta)=I_{F^2_{n_1}}(\theta)\dotplus\cdots\dotplus I_{F^2_{n_r}}(\theta),$$

同构映射 σ 由 (8) 给出. 此时，$\sigma(\alpha)=(\alpha_1,\cdots,\alpha_r)$，给出

$$\sum_{j=0}^{2^{n_1-3}-1}(\alpha_i^u)^j\equiv 0\ (\mathrm{mod}\ F_{n_i})$$

$$(i=1,\cdots,r,\ u=1,\cdots,2^{n_1+3}-1),$$

于是 $\alpha_1,\cdots,\alpha_r$ 分别给出 $I_{F^2_{n_i}}(\theta)$ 上的长为 2^{n_1+3} 的 DFT $(i=1,\cdots,r)$，故可分别在 $I_{F^2_{n_i}}(\theta)$ 上求出序列的卷积，再由 σ^{-1} 求出 $I_{M^2}(\theta)$ 上序列的卷积，这与第三章 §9 用孙子定理减少字长的道理是一样的.

应用定理 5 时，需先求出 $\alpha_1, \cdots, \alpha_r$，这可用定理 3 证明中的方法先求出 $GF(q_{k,i}^2)$ 中的 2^{n_1+3} 次本原单位根 $w_{k,i}$ $(k=1,\cdots,s_i)$，再求出 $I_{q_{k,i}^{2l_{k,i}}}(\theta)$ 的 N 次本原单位根 $\alpha_{k,i}=w_{k,i}^{q_{k,i}^{2(l_{k,i}-1)}}$ $(k=1,\cdots,s_i)$，由 $I_{F_{n_i}^2}(\theta)\simeq I_{q_{1,i}^{2l_{1,i}}}(\theta)\dotplus\cdots\dotplus I_{q_{s_{i,i}}^{2l_{s_{i,i}}}}(\theta)$ 的同构映射 σ，则 $\sigma^{-1}(\alpha_{1,i},\cdots,\alpha_{s_{i,i}})=\alpha_i$，即所求 $\alpha_i(i=1,\cdots,r)$。

至于一般的利用 $I_{q_i^{2l_i}}(\theta)$ 先算卷积，再用性质 2 求 $I_{M^2}(\theta)$ 中的卷积时，如何先求 $\alpha_i(i=1,\cdots,r)$，定理 3 的证明已给出一般算法，下面的例子就不具体计算 α_i 了。

例 1. 取 $R(\sqrt{3})$，其全体整数为 $a+b\sqrt{3}$，$a,b\in Z$，$N=32$，$x_i=a_i+b_i\sqrt{3}$，$h_i=c_i+d_i\sqrt{3}$，$\max(|a_i|,|b_i|)\leqslant 2^{10}$，$\max(|c_i|,|d_i|)\leqslant 2^8$，因[1] $2^3\cdot 2^5\cdot 2^{10}\cdot 2^8=2^{26}<F_2\cdot F_3\cdot F_4$，故可取 $M=F_2\cdot F_3\cdot F_4$，$\left(\frac{3}{F_2}\right)=\left(\frac{3}{F_3}\right)=\left(\frac{3}{F_4}\right)=-1$，由定理 5，可分别在 $I_{F_2^2}(\theta)$，$I_{F_3^2}(\theta)$，$I_{F_4^2}(\theta)$ 中求序列的卷积，字长由 F_4 定，即 32 位便可。

在应用方面，有实际意义的是求复整数的卷积。

例 2. 取 $R(i)$，$N=64$，$x_l=a_l+b_li$，$h_l=c_l+d_li$，$\max(|a_l|,|b_l|)\leqslant 2^{10}$，$\max(|c_l|,|d_l|)\leqslant 2^8$，因 $2^6\cdot 2^2\cdot 2^{10}\cdot 2^8=2^{26}$，$2^{19}<2^{26}<2^{31}$，直接用 §1 的方法，机器字长需 62 位，而用本节的方法可取 $M=(2^5-1)^3(2^7-1)^2$，需 30 位，或 $M=(2^7-1)^2(2^{13}-1)$，仅需 28 位，这不但可以减少字长，而且对 M 可有多种选择以适应计算机的字长。

---

1) $m\equiv 3\pmod 4$，在环 $I_{M^2}(\theta)$ 上计算 $R(\sqrt{m})$ 的整数的卷积时，还必须满足

$$\sum_{k=0}^{N-1}(|a_k||c_{\langle n-k\rangle_N}|+m|b_k||d_{\langle n-k\rangle_N}|)<\frac{M}{2},$$

和

$$\sum_{k=0}^{N-1}(|b_k||c_{\langle n-k\rangle_N}|+|a_k||d_{\langle n-k\rangle_N}|)<\frac{M}{2}.$$

§3. 在分圆域里计算卷积

为了计算分圆域里整数的卷积，与过去的方法相同，仍然是通过引入分圆域的整数剩余类环上的 DFT 来计算. 本节主要给出分圆域的整数剩余类环上 DFT 存在的充分必要条件、它的构造以及全部变换的个数.

1. 变换的构造

设 η 是复数域上的一个 n 次本原单位根，在第五章 §10 中，我们已经证明了域 $R(\eta)$ 是一个 $\varphi(n)$ 次的正规扩域，η 的定义多项式是分圆多项式

$$\varphi_n(x) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (x - \eta^i),$$

称 $R(\eta)$ 是 $\varphi(n)$ 次的分圆域，$1, \eta, \cdots, \eta^{\varphi(n)-1}$ 是 $R(\eta)$的一组整底，而且当 $\varphi_n(x)$ 模 q 不可约时，$[q]$ 是素理想数，这里 q 是有理素数. 于是，我们有

性质 1. 设 $M > 1$，M 是奇数，

$$I_{M^{\varphi(n)}}(\eta) = \left\{ \sum_{i=0}^{\varphi(n)-1} a_i \eta^i \,|\, a_i \in Z_M \ \ (i = 0, 1, \cdots, \varphi(n) - 1) \right\}, \quad (1)$$

在 (1) 中定义加法

$$\sum_{i=0}^{\varphi(n)-1} a_i \eta^i + \sum_{i=0}^{\varphi(n)-1} b_i \eta^i = \sum_{i=0}^{\varphi(n)-1} \langle a_i + b_i \rangle_M \eta^i \qquad (2)$$

和乘法

$$\sum_{i=0}^{\varphi(n)-1} a_i \eta^i \cdot \sum_{i=0}^{\varphi(n)-1} b_i \eta^i = \sum_{i=0}^{\varphi(n)-1} \langle r_i \rangle_M \eta^i, \qquad (3)$$

(3) 中 $f(x)g(x) = \varphi_n(x)q(x) + r(x)$，$f(x) = \sum\limits_{i=0}^{\varphi(n)-1} a_i x^i$，$g(x) = \sum\limits_{i=0}^{\varphi(n)-1} b_i x^i$，$r(x) = \sum\limits_{i=0}^{\varphi(n)-1} r_i x^i$，则对于运算 (2) 和 (3)，$I_{M^{\varphi(n)}}(\eta)$ 构

成一个有单位元素的、元素个数是 $M^{\varphi(n)}$ 的可换环. 如果 $M=q$ 是一个素数，$\varphi_n(x)$ 模 q 不可约，则 $I_{q^{\varphi(n)}}(\eta)$ 成域，此时记 $I_{q^{\varphi(n)}}(\eta)$ 为 $GF(q^{\varphi(n)})$.

与二次域的情况一样，我们常把环 $I_{M^{\varphi(n)}}(\eta)$ 叫做 $R(\eta)$ 的整数模 M 的剩余类环.

性质 2. 设 $M>1$，M 是奇数，$M=m_1\cdots m_r$，$(m_i, m_j)=1$ $(1\leqslant i<j\leqslant r)$，定义环 $I_{m_j^{\varphi(n)}}(\eta)$ $(j=1,\cdots,r)$ 的直和是

$$S_{M^{\varphi(n)}}(\eta)=I_{m_1^{\varphi(n)}}(\eta)\dotplus\cdots\dotplus I_{m_r^{\varphi(n)}}(\eta)$$
$$=\{(\alpha_1,\cdots,\alpha_r)\,|\,\alpha_j\in I_{m_j^{\varphi(n)}}(\eta)\ (j=1,\cdots,r)\},$$

在 $S_{M^{\varphi(n)}}(\eta)$ 中定义加法

$$(\alpha_1,\cdots,\alpha_r)+(\beta_1,\cdots,\beta_r)=(\alpha_1+\beta_1,\cdots,\alpha_r+\beta_r) \quad (4)$$

和乘法

$$(\alpha_1,\cdots,\alpha_r)(\beta_1,\cdots,\beta_r)=(\alpha_1\beta_1,\cdots,\alpha_r\beta_r), \quad (5)$$

则映射 ψ:

$$\psi\left(\sum_{i=0}^{\varphi(n)-1}a_i\eta^i\right)=\left(\sum_{i=0}^{\varphi(n)-1}\langle a_i\rangle_{m_1}\eta^i,\cdots,\sum_{i=0}^{\varphi(n)-1}\langle a_i\rangle_{m_r}\eta^i\right), \quad (6)$$

是 $I_{M^{\varphi(n)}}(\eta)$ 到 $S_{M^{\varphi(n)}}(\eta)$ 的同构映射.

性质 3. 设 q 是一个奇素数，$\varphi_n(x)$ 模 q 不可约，则有

1）同余式

$$f(x)=\sum_{i=0}^{n}c_ix^i\equiv 0\ (\mathrm{mod}\ q),$$
$$c_i\in Z(\eta)\ (i=0,1,\cdots,n), \quad (7)$$

在 $Z(\eta)$ 中解的个数 $\leqslant n$，重解计算在内，这里

$$Z(\eta)=\left\{\sum_{i=0}^{\varphi(n)-1}a_i\eta^i\,|\,a_i\in Z\ \ (i=0,1,\cdots,\varphi(n)-1)\right\},$$

解的个数是指非同余的解的个数.

2）如果 (7) 与 $f'(x)\equiv 0\ (\mathrm{mod}\ q)$ 无公解，则同余式

$$f(x)\equiv 0\ (\mathrm{mod}\ q^l)\quad (l\geqslant 1)$$

解的个数与 (7) 相同. 以上同余式的解均在 $Z(\eta)$ 上讨论.

设序列 x_i, $h_i\in I_{M^{\varphi(n)}}(\eta)$ $(i=0,1,\cdots,N-1)$，它们的循

环卷积是指

$$y_n = \sum_{k=0}^{N-1} x_k h_{\langle n-k \rangle_N} \quad (n = 0, 1, \cdots, N-1). \tag{8}$$

设变换

$$X_k = \sum_{n=0}^{N-1} x_n \alpha^{nk}, \ \alpha \in I_{M^{\varphi(n)}}(\eta) \ (k = 0, 1, \cdots, N-1) \tag{9}$$

有循环卷积性质

$$\sum_{n=0}^{N-1} x_n \alpha^{nk} \cdot \sum_{n=0}^{N-1} h_n \alpha^{nk} = \sum_{n=0}^{N-1} y_n \alpha^{nk} \quad (k = 0, 1, \cdots, N-1),$$

且有逆变换[1]，则称 (9) 给出的变换是 $I_{M^{\varphi(n)}}(\eta)$ 上一个长为 N 的 DFT.

用上一节类似的方法可证下面的定理.

定理 1. 设 $M = q_1^{l_1} \cdots q_r^{l_r}$, $\varphi_n(x)$ 模 q_i 不可约，q_i 是不同的奇素数 $(i = 1, \cdots, r)$，(9)是 $I_{M^{\varphi(n)}}(\eta)$ 上一个长为 N 的 DFT 的充分必要条件是 α_i 是环 $I_{q_i^{\varphi(n) l_i}}(\eta)$ 的 N 次单位根，且 α_i 是 $GF(q_i^{\varphi(n)})$ 的 N 次本原单位根 $(i = 1, \cdots, r)$，这里 $\psi(\alpha) = (\alpha_1, \cdots, \alpha_r)$ $\in S_{M^{\varphi(n)}}(\eta)$.

定理 2. 设 $M = q_1^{l_1} \cdots q_r^{l_r}$, $\varphi_n(x)$ 模 q_i 不可约，q_i 是不同的奇素数 $(i = 1, \cdots, r)$，存在 $I_{M^{\varphi(n)}}(\eta)$ 上长为 N 的 DFT 的充分必要条件是 $N \mid (q_1^{\varphi(n)} - 1, \cdots, q_r^{\varphi(n)} - 1)$.

定理 3. 设 $M = q_1^{l_1} \cdots q_r^{l_r}$, $\varphi_n(x)$ 模 q_i 不可约，q_i 是不同的奇素数 $(i=1, \cdots, r)$, $N \mid (q_1^{\varphi(n)} - 1, \cdots, q_r^{\varphi(n)} - 1)$，则 $I_{M^{\varphi(n)}}(\eta)$ 上长为 N 的 DFT 恰有 $\varphi^r(N)$ 个.

2. $\varphi_n(x)$ 模 q 不可约的充分必要条件

上节构造 DFT 时，用到条件 $\varphi_n(x)$ 模 q 不可约，自然会问，是否对每一个给定的 n，都存在素数 q，使分圆多项式 $\varphi_n(x)$ 模 q 不

---

1) 不难证明，其逆变换形如

$$x_n = N^{-1} \sum_{k=0}^{N-1} X_k \alpha^{-nk} \quad (n = 0, 1, \cdots, N-1),$$

其中，$NN^{-1} \equiv 1 \pmod M$.

可约？利用第五章 §10 中关于分圆域 $R(\eta)$ 上主理想数 $[q]$ 的分解结果可得下面的定理，它完全回答了这个问题.

定理. 设 q 是一个素数，n 阶分圆多项式 $\varphi_n(x)$ 模 q 不可约的充分必要条件是 $q\nmid n$，q 是模 n 的一个原根或 $q|n$，$q=2$，$n=2n_1$，$2\nmid n_1$，2 是 n_1 的一个原根.

证. 如果 $\varphi_n(x)$ 模 q 不可约，因为 $1, \eta, \cdots, \eta^{\varphi(n)-1}$ 是 $R(\eta)$ 的一组整底，显然 $\operatorname{index}\eta=1$，由第五章 §9 的定理 1 知 $[q]$ 为素理想数. 当 $q\nmid n$ 时，由第五章 §10 定理 2 知 $\frac{\varphi(n)}{h}=1$，即 $h=\varphi(n)$，q 是模 n 的一个原根. 当 $q|n$ 时，由第五章 §10 的定理 3 知，此时必须有 $\varphi(q^t)=1$，且 $\frac{\varphi(n_1)}{h}=1$，这就推出 $q=2$，$n=2n_1$，$2\nmid n_1$，2 是模 n_1 的一个原根.

反之，设 $q\nmid n$，q 是模 n 的一个原根，由第五章 §10 定理 2 知，$[q]$ 是 $R(\eta)$ 上的素理想数，再由第五章 §9 定理 1 知 $\varphi_n(x)$ 模 q 不可约. 或者当 $q|n$，$q=2$，$n=2n_1$，$2\nmid n_1$，2 是模 n_1 的一个原根，同理可证 $\varphi_n(x)$ 模 2 不可约.

推论 1. 设 p 是一个奇素数，$n=p^l$，$2p^l$ $(l\geqslant 1)$ 或 $n=4$，则存在无穷多个奇素数 q 使 $\varphi_n(x)$ 模 q 不可约.

证. 由第一章 §3.5 定理 1 知，此时 n 存在原根 v，且满足 $(v, 2n)=1$，而

$$2nk+v \quad (k=0, 1, \cdots), \tag{10}$$

均为 n 的原根，在 $(v, 2n)=1$ 时，级数 (10) 给出无穷多个奇素数 q，使 $\varphi_n(x)$ 模 q 不可约.

推论 2. 设 $n=p$ 是一个奇素数，p 的原根是素数 q 时，则

$$\varphi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

模 q 不可约.

这些推论告诉我们，分圆域的整数剩余类环上的 DFT 可大量构造出来.

下面给一个例子.

例．设 $n=5$，$M=q_1^{l_1}\cdots q_r^{l_r}$，素数 $q_i=2^{\lambda_i}-1$，λ_i 是形如 $4t+3$ 的素数（$i=1,\cdots,r$），$\lambda_1<\lambda_2<\cdots<\lambda_r$，由于 2 是模 5 的原根，所以 $q_i\equiv 2\ (\mathrm{mod}\ 5)$（$i=1,\cdots,r$）都是模 5 的原根，而 $x^4+x^3+x^2+x+1$ 模 q_i 不可约（$i=1,\cdots,r$），故可构造出长为 $N(N|(q_1^4-1,\cdots,q_r^4-1))$ 的 $I_{M^4}(\eta)$ 上的 DFT，当序列的长度是 2 的方幂时，可卷积的最大长度是 $N=2^{\lambda_1+2}$。

3. 关于实分圆域

设 η 是一个 n 次本原单位根，$R(\eta+\eta^{-1})$ 是 $R(\eta)$ 的最大实子域，称实分圆域，其次数为 $\frac{\varphi(n)}{2}$，这里 $n>2$。于是，$\eta+\eta^{-1}$ 满足一个首项系数为 1 的、次数为 $\frac{\varphi(n)}{2}$ 的、有理整数的不可约多项式．我们来证明下面的定理．

定理 1．设 $n>2$，$F_n(x)=\prod\limits_{i=1}^{\frac{\varphi(n)}{2}}(x-\eta^{k_i}-\eta^{n-k_i})$，$1\leqslant k_1<k_2<\cdots<k_{\varphi(n)}<n$，$(k_i,n)=1$（$i=1,\cdots,\varphi(n)$），则 $F_n(x)$ 是 $\eta+\eta^{-1}$ 在 R 上的定义多项式．

证．$(k_i,n)=1$，则 $(n,n-k_i)=1$（$i=1,\cdots,\varphi(n)$），且 $n-k_{\varphi(n)}=k_1$，$n-k_{\varphi(n)-1}=k_2$，$n-k_{\varphi(n)-2}=k_3$，$\cdots$，$n-k_1=k_{\varphi(n)}$，一般地，可表示为 $n-k_i=k_j$，$i+j=\varphi(n)+1$，$1\leqslant i,j\leqslant\varphi(n)$，$\eta$ 在 R 上 $\varphi(n)$ 个共轭数可设为 $\eta^{(1)}=\eta$（$k_1=1$），$\eta^{(2)}=\eta^{k_2}$，$\cdots$，$\eta^{(\varphi(n))}=\eta^{k_{\varphi(n)}}$，设 $\rho=\eta+\eta^{-1}=\eta+\eta^{n-1}$，$\rho$ 在 R 上的共轭数为 $\rho^{(i)}=\eta^{(i)}+\eta^{(i)n-1}=\eta^{k_i}+\eta^{k_i(n-1)}=\eta^{k_i}+\eta^{n-k_i}$（$i=1,\cdots,\varphi(n)$），而 $\rho^{(i)}=\rho^{(\varphi(n)+1-i)}\left(i=1,\cdots,\frac{\varphi(n)}{2}\right)$，于是由第五章 §2 定理 5 知 $F_n(x)$ 是 $\rho=\eta+\eta^{-1}$ 在 R 上的定义多项式．

由于 $1,\rho,\cdots,\rho^{\frac{\varphi(n)}{2}-1}$ 是 $R(\rho)$ 的一组整底，设 $M>1$，M 是奇数，设

$$I_{M^{\frac{\varphi(n)}{2}}}(\rho)=\left\{\sum_{i=0}^{\frac{\varphi(n)}{2}-1}a_i\rho^i\,|\,a_i\in Z\ \left(i=0,1,\cdots,\frac{\varphi(n)}{2}-1\right)\right\},$$

类似上节的运算(2)和(3)，可证明 $I_M^{\frac{\varphi(n)}{2}}(\rho)$ 成环，叫 $R(\rho)$ 的整数模M的剩余类环．这样一来，可类似地定义环 $I_M^{\frac{\varphi(n)}{2}}(\rho)$ 上的DFT，上一节的全部性质和定理，可用同样的方法推出，例如能够证明下面的定理．

定理 2．设 $M = q_1^{l_1}\cdots q_r^{l_r}$，$F_n(x)$ 模 q_i 不可约，q_i 是不同的奇素数 $(i = 1, \cdots, r)$，存在 $I_M^{\frac{\varphi(n)}{2}}(\rho)$ 上长为N的 DFT 的充分必要条件是 $N|(q_1^{\frac{\varphi(n)}{2}} - 1, \cdots, q_r^{\frac{\varphi(n)}{2}} - 1)$．

此外，因为 $R(\rho)$ 是 $R(\eta)$ 的子域，所以$[q]$(q 是有理素数)是 $R(\eta)$ 上的素理想数，则一定也是 $R(\rho)$ 上的素理想数．于是，若 $\varphi_n(x)$ 模 q 不可约，则 $[q]$ 是 $R(\eta)$ 上的素理想数，因而 $[q]$ 也是 $R(\rho)$ 上的素理想数，再由第五章§9的定理可知对于这样的q，有 $F_n(x)$ 模 q 不可约．这就证明了下一个定理．

定理 3．设 $n > 2$，q 是一个有理素数，如果 $\varphi_n(x)$ 模 q 不可约，则 $F_n(x)$ 也模 q 不可约．

4．关于一般的代数数域

前面，我们完全解决了二次域和分圆域的整数剩余类环上的DFT 存在的充分必要条件、算法和个数，那么在一般的代数数域 $R(\theta)$ 里又如何呢？前面的证明依赖于二次域的整底 $1, \sqrt{m}$ $\left(或 1, \dfrac{\sqrt{m}+1}{2}\right)$ 和分圆域 $R(\eta)$ 的整底 $1, \eta, \cdots, \eta^{\varphi(n)-1}$ 的形状，而在一般的代数数域中，有时这样形状的整底根本不存在．然而，利用 $R(\theta)$ 的任一组整底 $\alpha_1, \cdots, \alpha_n$ 和有关主理想数 $[q]$ (q 是有理素数)分解的结果，仍然可以把前面的全部结果推广到任意的代数数域上去，这里就不详述了．有兴趣的读者可查阅书后所附的有关文献．

第七章　任意环上具有循环卷积性质的可逆变换

§1. 引　　言

在第二,三,六章中,我们曾分别讨论了复数域上、整数模M的剩余类环上、二次域和分圆域中整数剩余类环上计算卷积的问题. 本章里,我们将讨论在任意抽象环上计算卷积的问题,以期使读者对各种具体环上的 DFT 构造有一个系统的全面的认识.

从前面的讨论知道,各种环(复数域自然也是一个环)上的 DFT 型变换均具有两条重要的性质,即有所谓"循环卷积性质"和有逆变换存在. 反之,容易看出,凡具有这两条性质的变换(本章中将简记为 CRT)便均可用来计算两个序列的卷积(自然,它们不一定可进行类似 FFT 的快速演段).

我们知道,在复数域上,具有循环卷积性质的可逆变换必为 DFT,亦即在复数域上 DFT 是 CRT 的唯一构造. 因此,我们自然会问,数论变换(即环 Z_M 上的 DFT)是否也是环 Z_M 上之 CRT 的唯一构造呢? 一般地,是否在任意环上凡具有循环卷积性质的可逆变换均必为 DFT 型变换呢? 亦即,是否在任意环上,DFT 构造也是其上之 CRT 的唯一构造呢? 若否,那么两者之间的相互关系如何呢? 它们各自存在的充分必要条件是什么呢? CRT 及其逆变换的一般构造又是什么样子呢? 在本章中,我们将对这些问题给予一般性的解决,并以环 Z_M 为例进行具体的剖析.

§2. 任意环上的 CRT

本节中,如无特殊声明,概以 R 表示任意一个有单位元素的交

换环(有限或无限均可). 因为复数域,环 Z_M 和二次域、分圆域中的整数剩余类环都是有单位元素的交换环，故本节所得的全部结果对于它们均能成立.

环 R 上一个矩阵为 T、长为 N 的变换是指由下式

$$\vec{X} = T\vec{x}$$

所确定的变 R 中任意长为 N 的序列 $\vec{x}$ 为 R 中另一长为 N 的序列 $\vec{X}$ 的一个变换,这里

$$\vec{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}, \quad \vec{X} = \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{N-1} \end{pmatrix}, \quad T = \begin{pmatrix} t_{0,0} \cdots t_{0,N-1} \\ t_{1,0} \cdots t_{1,N-1} \\ \cdots\cdots\cdots\cdots \\ t_{N-1,0} \cdots t_{N-1,N-1} \end{pmatrix},$$

$x_i, X_i, t_{i,j} \in R$ $(i, j = 0, 1, \cdots, N-1)$.

环 R 上一个矩阵为 T、长为 N 的变换具有所谓“循环卷积性质”,是指对 R 中任意两个长为 N 的序列 $\vec{x}$, $\vec{h}$ 和它们的循环卷积

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \vec{y} = \vec{x} * \vec{h} = \begin{pmatrix} h_0 h_{N-1} & \cdots h_1 \\ h_1 h_0 & \cdots h_2 \\ \cdots\cdots\cdots\cdots \\ h_{N-1} h_{N-2} & \cdots h_0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix},$$

即

$$y_k = \sum_{n=0}^{N-1} x_n h_{\langle k-n \rangle_N} \quad (k = 0, 1, \cdots, N-1).$$

若令

$$\vec{X} = T\vec{x}, \quad \vec{Y} = T\vec{y}, \quad \vec{H} = T\vec{h},$$

则常有

$$Y_k = H_k \cdot X_k \quad (k = 0, 1, \cdots, N-1).$$

为方便起见,引入下之:

定义 1. 环 R 上一个长为 N 的具有循环卷积性质的可逆变换称为环 R 上一个长为 N 的 CRT.

一个主要的定理是下面的:

定理 1. 环 R 上矩阵为 T、长为 N 的 CRT 存在的充分必要条件是,存在元素 $\alpha_i \in R$ $(i = 0, 1, \cdots, N-1)$ 适合

i) $$T=\begin{pmatrix}1 & \alpha_0 & \cdots & \alpha_0^{N-1}\\ 1 & \alpha_1 & \cdots & \alpha_1^{N-1}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha_{N-1} & \cdots & \alpha_{N-1}^{N-1}\end{pmatrix}; \tag{1}$$

ii) $\alpha_i^N=1 \quad (i=0, 1, \cdots, N-1)$;

iii) 对 $0\leqslant i<j\leqslant N-1$，$\alpha_j-\alpha_i$ 的逆元素均存在。

证．设变换矩阵为

$$T=\begin{pmatrix}t_{0,0} & \cdots & t_{0,N-1}\\ t_{1,0} & \cdots & t_{1,N-1}\\ \cdots & \cdots & \cdots\\ t_{N-1,0} & \cdots & t_{N-1,N-1}\end{pmatrix}, \quad t_{i,j}\in R \ (i, j=0, 1, \cdots, N-1).$$

则由循环卷积性质知，对 R 中任意两个长为 N 的序列 x_n，h_n 和它们的循环卷积 y_n ($n=0, 1, \cdots, N-1$) 均应有

$$\left(\sum_{n=0}^{N-1} t_{k,n}x_n\right)\left(\sum_{m=0}^{N-1} t_{k,m}h_m\right)=\sum_{l=0}^{N-1} t_{k,l}y_l,$$

即

$$\sum_{n=0}^{N-1}\sum_{m=0}^{N-1} t_{k,n}t_{k,m}x_nh_m=\sum_{r=0}^{N-1} x_r\sum_{l=0}^{N-1} t_{k,l}h_{\langle l-r\rangle_N}$$
$$(k=0, 1, \cdots, N-1).$$

今先取定 $(x_0, \cdots, x_{N-1})=(0, 1, 0, \cdots, 0)$，再顺次取 $(h_0, \cdots, h_{N-1})=(1, 0, 0, \cdots, 0)$; $(0, 1, 0, \cdots, 0)$; $\cdots$; $(0, \cdots, 0, 1)$，这里的 0 和 1 分别表示环 R 中的零元素和单位元素．即可得到

$$\begin{cases} t_{k,1}\cdot t_{k,0}=\sum\limits_{l=0}^{N-1} t_{k,l}h_{\langle l-1\rangle_N}=t_{k,1},\\ t_{k,1}\cdot t_{k,1}=\sum\limits_{l=0}^{N-1} t_{k,l}h_{\langle l-1\rangle_N}=t_{k,2},\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ t_{k,1}\cdot t_{k,N-2}=\sum\limits_{l=0}^{N-1} t_{k,l}h_{\langle l-1\rangle_N}=t_{k,N-1},\\ t_{k,1}\cdot t_{k,N-1}=\sum\limits_{l=0}^{N-1} t_{k,l}h_{\langle l-1\rangle_N}=t_{k,0}\end{cases}$$

($k=0,1,\cdots,N-1$). 由此立刻得到

$$\begin{cases} t_{k,n}=t_{k,1}^{n}, & (2\leqslant n\leqslant N-1) \\ t_{k,0}=t_{k,1}^{N}, \\ t_{k,1}=t_{k,1}^{N+1}. \end{cases} \tag{2}$$

因此,若记 $t_{k,1}=\alpha_k$ ($k=0,1,\cdots,N-1$), 则得

$$T=\begin{pmatrix} \alpha_0^N\alpha_0 & \cdots & \alpha_0^{N-1} \\ \alpha_1^N\alpha_1 & \cdots & \alpha_1^{N-1} \\ \cdots\cdots & \cdots & \cdots\cdots \\ \alpha_{N-1}^N\alpha_{N-1} & \cdots & \alpha_{N-1}^{N-1} \end{pmatrix},$$

从而知行列式

$$|T|=\alpha_0\cdot\alpha_1\cdots\alpha_{N-1}\cdot\alpha,\quad \alpha\in R.$$

又因 T^{-1} 存在,故 $|T|^{-1}$ 亦应存在,从而知 α_k^{-1} ($k=0,1,\cdots,N-1$) 存在. 于是由 (2) 可得 $\alpha_k^N=1$ ($k=0,1,\cdots,N-1$) 且 T 合 (1). 由 (1) 知

$$|T|=\prod_{0\leqslant i<j\leqslant N-1}(\alpha_j-\alpha_i),$$

再由 T^{-1} 存在知 $(\alpha_j-\alpha_i)^{-1}$ 存在. 必要性已得到证明.

今若定理之条件成立,则由 i)、iii)知 T^{-1}存在,所以变换可逆.

又对任意整数 k ($0\leqslant k\leqslant N-1$), 由 ii) 知

$$\begin{aligned} Y_k &= \sum_{m=0}^{N-1}\alpha_k^m y_m=\sum_{j=0}^{N-1}x_j\sum_{m=0}^{N-1}\alpha_k^m h_{\langle m-j\rangle_N} \\ &= \sum_{j=0}^{N-1}x_j\alpha_k^j\sum_{m=0}^{N-1}\alpha_k^{m-j}h_{\langle m-j\rangle_N} \\ &= \sum_{j=0}^{N-1}x_j\alpha_k^j\sum_{m=0}^{N-1}\alpha_k^{\langle m-j\rangle_N}h_{\langle m-j\rangle_N} \\ &= \sum_{j=0}^{N-1}x_j\alpha_k^j\sum_{n=0}^{N-1}\alpha_k^n h_n=X_k\cdot H_k. \end{aligned}$$

故条件充分. 至此定理全部证毕.

定义 2. 环 R 上矩阵有形状

$$T=\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha & \cdots & \alpha^{N-1}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{N-1} & \cdots & \alpha^{(N-1)2}\end{pmatrix} \tag{3}$$

的一个长为N的 CRT 称为环R上一个长为N的 DFT.

由此可知,环R上的 DFT 只是环R上的一类特殊的CRT. 还应指出的是,与前面讨论各类 DFT 时所给出的定义相比,定义 2 中没有把关于逆 DFT 的具体构造作为要求写入. 因由下面的定理 2 知道,这一要求是不独立的.

定理 2. 在环R上,若长为N之 CRT 存在,则必 N^{-1} 存在,且(1) 之唯一的逆矩阵为

$$T^{-1}=N^{-1}\begin{pmatrix}1 & 1 & \cdots & 1\\ \alpha_0^{-1} & \alpha_1^{-1} & \cdots & \alpha_{N-1}^{-1}\\ \cdots & \cdots & \cdots & \cdots\\ \alpha_0^{-(N-1)} & \alpha_1^{-(N-1)} & \cdots & \alpha_{N-1}^{-(N-1)}\end{pmatrix}. \tag{4}$$

证. 由定理 1 之条件 ii) 知,若令

$$f_1(x)=x^{N-1}+\alpha_0x^{N-2}+\cdots+\alpha_0^{N-2}x+\alpha_0^{N-1},$$

则有

$$x^N-1=(x-\alpha_0)f_1(x)+\alpha_0^N-1=(x-\alpha_0)f_1(x).$$

再由定理 1 条件 ii)、iii) 知, $\alpha_1,\cdots,\alpha_{N-1}$ 必均为 $f_1(x)$ 之根. 故又可得

$$f_1(x)=(x-\alpha_1)f_2(x).$$

如此经N步后可得

$$x^N-1=(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{N-1}) \tag{5}$$

和

$$f_1(x)=(x-\alpha_1)\cdots(x-\alpha_{N-1}). \tag{6}$$

于是, 由 (6) 及 $(\alpha_j-\alpha_0)^{-1}$ $(j=1,2,\cdots,N-1)$ 存在便知

$$N^{-1}=\alpha_0^{N-1}\prod_{1\leqslant j\leqslant N-1}(\alpha_0-\alpha_j)^{-1}$$

存在.

又由 (5) 可知

$$\sigma_1=\sigma_2=\cdots=\sigma_{N-1}=0,\qquad \sigma_N=(-1)^{N+1},\tag{7}$$

这里, σ_l 表示 $\alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ 的初级对称多项式 ($l=1, 2, \cdots, N$).

欲证 (4) 为 (1) 之逆,只需证 $0\leqslant i, j\leqslant N-1$ 时

$$N^{-1}\sum_{k=0}^{N-1}\alpha_k^{-i}\cdot\alpha_k^{j}=N^{-1}\sum_{k=0}^{N-1}\alpha_k^{j-i}=\begin{cases}1, & \text{当 } i=j,\\ 0, & \text{当 } i\neq j.\end{cases}$$

$i=j$ 时是显然的. $i\neq j$ 时,若 $i>j$, 以 $N+j-i$ 代替 $j-i$ 即知,只需证明 $1\leqslant l\leqslant N-1$ 时

$$S_l=\sum_{k=0}^{N-1}\alpha_k^l=0\tag{8}$$

即可. 而由 $1\leqslant l\leqslant N-1$ 时之等次和的牛顿公式

$$S_l-S_{l-1}\sigma_1+S_{l-2}\sigma_2-\cdots+(-1)^{l-1}S_1\sigma_{l-1}+(-1)^l l\sigma_l=0$$

及 (7) 式便知 (8) 成立. 定理证毕.

由定理 1 和定理 2 及定义 2 立刻得到下面的结论:

推论 1. 环 R 上长为 N 之 DFT 存在的充分必要条件为, 存在 $\alpha\in R$, 适合

i) $\alpha^N=1$;

ii) 对 $1\leqslant r\leqslant N-1$, α^r-1 之逆元素存在.

推论 2. 在环 R 上,若有长为 N 之 DFT 存在,则必有 N^{-1} 存在,且其逆变换之矩阵为

$$T^{-1}=N^{-1}\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \alpha^{-1} & \cdots & \alpha^{-(N-1)}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha^{-(N-1)} & \cdots & \alpha^{-(N-1)^2}\end{pmatrix}.$$

在下节中将看到,一般情形下,环 R 上若有长为 N 之 CRT 存在,则其中既有 DFT. 更有大量非 DFT 的 CRT. 为进一步弄清环 R 上之 CRT 与 DFT 的相互关系,我们引入下面的定义.

定义 3. 若环 R 上两个长为 N 之 CRT 的矩阵可只经过行的有

限次调换而由此得彼，亦即，若构成此二 CRT 之两组 $\alpha_0, \alpha_1, \cdots,$ α_{N-1} 所成之两个N元集相同，则称此二 CRT 是同集的。

于是，下面的定理成立

定理 3. 对给定的正整数N，若在环R中二项方程

$$x^N - 1 = 0 \tag{9}$$

之根数不超过N，则R上任一长为N的 CRT 均与R上一长为N的 DFT 同集。即若不计变换矩阵之行的顺序差异，此时R上长为N的 DFT 是R上长为N的 CRT 的唯一构造。

证. 设 (1) 是环R上长为N的任一个 CRT，则由定理 1 条件 ii)，iii) 及本定理之假设可知，$\alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ 为方程 (9) 之全部根。

今设 $N = p_1^{r_1} \cdots p_s^{r_s}$，则对任意 k，$1 \leqslant k \leqslant s$，显然方程

$$x^{\frac{N}{p_k}} - 1 = 0 \tag{10}$$

之根均为 (9) 之根. 又方程 (9)、(10) 显然均无重根，因此，在 $\alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ 中必可找到 (10) 之全部根，设其为 $\alpha_1', \alpha_2', \cdots,$ α_{N_k}'，$\alpha_i' \in \{\alpha_0, \alpha_1, \cdots, \alpha_{N-1}\}$ $(1 \leqslant i \leqslant N_k \leqslant N-1)$。

如果 $N_k > \dfrac{N}{p_k}$，则由定理 1 条件 iii) 及定理 2 之证明可得

$$x^{\frac{N}{p_k}} - 1 = (x - \alpha_1') \cdots (x - \alpha_{N/p_k}'),$$

从而可得

$$0 = (\alpha_{N/p_k+1}' - \alpha_1') \cdots (\alpha_{N/p_k+1}' - \alpha_{N/p_k}').$$

因 $\alpha_i' \in \{\alpha_0, \cdots, \alpha_{N-1}\}$，将由定理 1 条件 iii) 将得到 $0 = 1$ 这一矛盾结果，因而 $N_k \leqslant \dfrac{N}{p_k} < N$ 必成立。

所以，在 $\alpha_0, \cdots, \alpha_{N-1}$ 中至少有一个，记为 β_k，且适合

$$\beta_k^{N/p_k} - 1 \neq 0.$$

由此易证 $\beta_k^{N/p_k^{r_k}} = \gamma_k \in \{\alpha_0, \cdots, \alpha_{N-1}\}$ 之阶为 $p_k^{r_k}$. 进而可证 $\alpha = \prod_{k=1}^{s} \gamma_k \in \{\alpha_0, \cdots, \alpha_{N-1}\}$ 之阶为N. 至此已经证明了在 $\alpha_0, \cdots,$ α_{N-1} 中必有阶为N之α存在，例如 $\alpha = \alpha_0$，则 $\alpha_0^0, \alpha_0^1, \cdots, \alpha_0^{N-1}$ 互

不相同且均为(9)之根，故$\{\alpha_0^0, \alpha_0^1, \cdots, \alpha_0^{N-1}\}=\{\alpha_0, \alpha_1, \cdots, \alpha_{N-1}\}$，从而适当调换$T$之行的顺序后，$T$即具有(3)之形状．证毕．

推论 3．当R取作

i) 任意域；

ii) p为奇素数时，模p^l之剩余类环Z_{p^l}；

iii) 有单位元素之整环；

iv) m无平方因子，Legendre 符号$\left(\frac{m}{p}\right)=-1$时，二次域$R(\sqrt{m})$中的代数整数模$p^l$之剩余类环$I_{p^{2l}}(\theta)$，这里

$$\theta=\begin{cases}\sqrt{m}, & \text{当 } m\equiv 2, 3 \pmod 4),\\ \frac{1}{2}(1+\sqrt{m}), & \text{当 } m\equiv 1 \pmod 4).\end{cases}$$

之一时，R上之 CRT 均同集于R上之 DFT．

证．i),ii),iii)适合定理条件是熟知的．iv)适合定理条件已见第五章．

§ 3. Z_M上的 CRT

本节中将着重讨论R取作模M之剩余类环Z_M的情形．此时易将§2节中的定理1和推论1改述为

定理 1′．设$M=p_1^{l_1}\cdots p_s^{l_s}$，则环$Z_M$上长为$N$之 CRT 存在的充分必要条件为，存在整数$\alpha_0, \alpha_1, \cdots, \alpha_{N-1}\in Z_M$，适合

i) 变换矩阵T具有(1)之形状；

ii) $\alpha_i^N\equiv 1 \pmod M$　$(i=0, 1, \cdots, N-1)$；

iii) $0\leqslant i<j\leqslant N-1$时，$(\alpha_j-\alpha_i, p_k)=1$　$(k=1, 2, \cdots, s)$．

推论 1′．Z_M上长为N之 DFT (即 NTT) 存在的充分必要条件为存在整数$\alpha\in Z_M$，适合

i) $\alpha^N\equiv 1 \pmod M$；

ii) α模p_k之次数为N　$(k=1, 2, \cdots, s)$．

由定理1′知，若$2|M$，则由ii)知，$\alpha_0, \cdots, \alpha_{N-1}$全为奇数．而

由 iii) 知，当 $0 \leqslant i < j \leqslant N-1$ 时，$(\alpha_j - \alpha_i, 2) = 1$. 当 $N > 1$ 时这是不可能的，故必 $N = 1$. 因此，我们在讨论 Z_M 上的 CRT 时均假定 M 为奇数.

由推论 1′ 条件 ii) 知，$N | O(M) = (p_1 - 1, \cdots, p_s - 1)$. 反之，由 $N | O(M)$ 知 $N | p_k - 1 (k = 1, 2, \cdots, s)$, 故存在 β_k 模 p_k 的次数为 N, 从而存在 $\alpha_k = \beta_k^{p_k^{l_k - 1}}$ 模 $p_k^{l_k}$ 的次数为 N（见第三章 § 2). 再由孙子定理知存在 $\alpha \equiv \alpha_k \pmod{p_k^{l_k}} (k = 1, 2, \cdots, s)$ 适合推论 1′ 之条件 i), ii). 这就得出了关于 NTT 的一个已知结果，即下之:

推论 4. Z_M 上长为 N 之 DFT 存在的充分必要条件为 $N | O(M)$.

对 Z_M 这一特定的环来说，我们可进一步证明推论 4 对 CRT 亦是成立的，即有下面的定理.

定理 4. Z_M 上长为 N 之 CRT 存在的充分必要条件为 $N | O(M)$.

证. 因 DFT 是一类特殊的 CRT, 故由推论 4 知，条件是充分的.

今设 Z_M 上长为 N 之 CRT 存在，则由定理 1′ 知，有 $\alpha_0, \alpha_1, \cdots, \alpha_{N-1} \in Z_M$, 适合定理 1′ 的条件 ii), iii). 由此可知 $\alpha_0, \alpha_1, \cdots, \alpha_{N-1}$ 是方程

$$x^N - 1 \equiv 0 \pmod{p_k} \quad (1 \leqslant k \leqslant s)$$

之 N 个互不同余的解.

设 $p_k - 1 = q_k N + r_k \quad (1 \leqslant k \leqslant s, \ 0 \leqslant r_k < N)$. 则由 $\alpha_i^{p_k - 1} = (\alpha_i^N)^{q_k} \cdot \alpha_i^{r_k}$ 知

$$\alpha_i^{r_k} - 1 \equiv 0 \pmod{p_k},$$

$1 \leqslant k \leqslant s \ (i = 0, 1, \cdots, N-1)$. 这就说明方程

$$x^{r_k} - 1 \equiv 0 \pmod{p_k}$$

有 N 个互不同余的解. 但该方程在 $r_k \geqslant 1$ 时最多只有 r_k 个解，故由 $0 \leqslant r_k < N$ 知 $r_k = 0$, 亦即 $N | p_k - 1$, $1 \leqslant k \leqslant s$, 故条件必要. 证毕.

由推论 3 知，存在 M，使 Z_M 上全部 CRT 均同集于 DFT. 但由定理 4 和推论 4 知，不存在 M，使 Z_M 上全部 CRT 均非 DFT.

对于环 Z_M，我们还可更进一步算出其上长为 N 之全部 CRT 的个数. 对此有下面的定理.

定理 5. *若 $N|O(M)$，则 Z_M 上共有 $(N!)^s$ 个不同的 CRT.*

证. 因 Z_M 上之 CRT 与合定理 1′ 条件 ii), iii) 之 N 元序列 $(\alpha_0, \alpha_1, \cdots, \alpha_{N-1})$ 是一一对应的. 因此，只需求出这样的 N 元序列的个数即可.

由 $N|O(M)$ 知，对任意 i，$1 \leqslant i \leqslant s$，模 p_i 次数为 N 之数 γ_i 存在. 若令 $g_i = \gamma_i^{p_i^{l_i-1}}$，则由第三章 § 2 知，$g_i$ 模 p_i 和模 $p_i^{l_i}$ 之次数均为 N. 于是，$\gamma_i^0, \gamma_i^1, \cdots, \gamma_i^{N-1}$ 和 $g_i^0, g_i^1, \cdots, g_i^{N-1}$ 分别表示同余方程

$$x^N - 1 \equiv 0 \pmod{p_i}$$

和

$$x^N - 1 \equiv 0 \pmod{p_i^{l_i}}$$

之 N 个互不同余的解. 但上面两个方程之解数均不能超过 N，故它们分别表示上面两个方程的全部解. 由此，用孙子定理易证，方程

$$x^N - 1 \equiv 0 \pmod{M}$$

有且仅有 N^s 个解 $\alpha_{g_1^{j_1}, \cdots, g_s^{j_s}}$，$0 \leqslant j_k \leqslant N-1$，$1 \leqslant k \leqslant s$，这里，$\alpha_{g_1^{j_1}, \cdots, g_s^{j_s}}$ 表示同余式组

$$\begin{cases} x \equiv g_1^{j_1} \pmod{p_1^{l_1}}, \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv g_s^{j_s} \pmod{p_s^{l_s}} \end{cases}$$

模 M 之唯一解.

由此 N^s 个 α，显然能且只能作成 $A_{N^s}^N = \dfrac{(N^s)!}{(N^s - N)!}$ 个不同的 N 元序列 $(\alpha_0, \alpha_1, \cdots, \alpha_{N-1})$. 所以，它们是适合定理 1′ 条件 ii) 的全部可能的 N 元序列.

下面只需进一步证明，在这 $A_{N^s}^N$ 个 N 元序列中，合定理 1′ 条

件 iii）者恰有$(N!)^s$个即可．为此，设N元序列$(\alpha_0, \alpha_1, \cdots, \alpha_{N-1})$之元素为

$$\alpha_k = \alpha_{g_1^{j_{1,k}}, \cdots, g_s^{j_{s,k}}},$$

$0 \leqslant j_{i,k} \leqslant N-1$ $(i = 1, 2, \cdots, s;\ k = 0, 1, \cdots, N-1)$．即设

$$\alpha_k \equiv g_i^{j_{i,k}} \pmod{p_i^{l_i}}$$

$(i = 1, 2, \cdots, s;\ k = 0, 1, \cdots, N-1)$．

因

$$g_i \equiv \gamma_i \pmod{p_i} \quad (i = 1, 2, \cdots, s),$$

故得

$$\alpha_k \equiv \gamma_i^{j_{i,k}} \pmod{p_i}$$

$(i = 1, 2, \cdots, s;\ k = 0, 1, \cdots, N-1)$．

所以，如果N元序列$(\alpha_0, \alpha_1, \cdots, \alpha_{N-1})$适合定理 1′ 条件 iii)，则必$j_{i,0}, j_{i,1}, \cdots, j_{i,N-1}$中无二者相等．又$0 \leqslant j_{i,k} \leqslant N-1$ $(k = 0, 1, \cdots, N-1)$，故必$j_{i,0}, j_{i,1}, \cdots, j_{i,N-1}$为$0, 1, \cdots, N-1$的一个排列．反之，若对$i = 1, 2, \cdots, s$，$j_{i,0}, j_{i,1}, \cdots, j_{i,N-1}$都是$0, 1, \cdots, N-1$的一个排列时，由$\alpha_k = \alpha_{g_1^{j_{1,k}}, \cdots, g_s^{j_{s,k}}}$所得出的$N$元序列$(\alpha_0, \alpha_1, \cdots, \alpha_{N-1})$必满足定理 1′ 的条件 ii), iii)．因此，适合定理 1′条件ii), iii)的N元序列之个数应等于由$0, 1, \cdots, N-1$这N个数所作成之不同排列的个数的s次幂，即$(N!)^s$．证毕．

容易验证定义 3 所规定的环R上 CRT 之间的同集关系具有反身、对称、传递的性质．故可依此关系将R上之全部长为N的CRT进行分类，同类者皆相互同集，异类者皆互不同集．我们简称这样的类为同集类．由定义 3 知，同类的全部 CRT，其矩阵间均只有行的顺序之差异．而从任一个 CRT 之矩阵出发，通过调换行的顺序，显然共可得到$N!$个不同的矩阵，它们分别对应着$N!$个相互不同但相互同集的 CRT．故每一同集类中均有且仅有$N!$个互不相同的 CRT．于是，由定理 5 立刻可得：

推论 5． 若$N|O(M)$，则Z_M上全部 CRT 共可分为$(N!)^{s-1}$个同集类．

如前所述，在一般情况下，当 $N|O(M)$ 时，Z_M 上可能同时有 DFT 和非 DFT 之 CRT 存在. 今进而考虑在上述 $(N!)^{s-1}$ 个同集类中 DFT 的分布情况如何？对此有下面的定理.

定理 6. 若 $N|O(M)$，则 Z_M 上任一同集类中所含 DFT 之个数为 0 或 $\varphi(N)$，这里，$\varphi(N)$ 表示 Euler 函数.

证. 显然只需证明，对任意给定的 DFT，有且只有 $\varphi(N)$ 个(包括它自身在内)不同的 DFT 与之同集就够了. 因 Z_M 上长为 N 之 CRT 与适合推论 1′ 条件 i)，ii) 之 α 是一一对应的，故又只需证明，在适合推论 1′ 条件的全部 α 中，对任一给定的 α，有且只有 $\varphi(N)$ 个 α' (包括 α 本身在内)使 N 元集 $\{\alpha'^0, \alpha'^1, \cdots, \alpha'^{N-1}\}$ 等于 N 元集 $\{\alpha^0, \alpha^1, \cdots, \alpha^{N-1}\}$ 就够了.

由推论 1′ 条件 i)，ii) 易知，α 模 M 之次数亦为 N，故 $\alpha^0, \alpha^1, \cdots, \alpha^{N-1}$ 构成一个循环群. 熟知，当 $0 \leqslant k \leqslant N-1$，$(k, N)=1$ 时，α^k 互不相同，且均为此群之生成元素. 这样的 α^k (包括 $\alpha=\alpha'$ 在内)显然共有 $\varphi(N)$ 个，它们均合所求.

反之，设 α' 与 α 所对应之 DFT 同集，则由 N 元集 $\{\alpha'^0, \alpha'^1, \cdots, \alpha'^{N-1}\} = \{\alpha^0, \alpha^1, \cdots, \alpha^{N-1}\}$ 知，必有 n，$1 \leqslant n \leqslant N-1$，存在，使 $\alpha' \equiv \alpha^n \pmod M$.

于是，

$$\alpha'^{\frac{N}{(n,N)}} \equiv \alpha^{\frac{n}{(n,N)}N} \equiv 1 \pmod M.$$

从而

$$\alpha'^{\frac{N}{(n,N)}} \equiv 1 \pmod{p_i} \quad (1 \leqslant i \leqslant s).$$

故由推论 1′ 条件 ii) 可得 $N \Big| \dfrac{N}{(n, N)}$，所以 $(n, N)=1$，即 α' 必与上述 $\varphi(N)$ 个 α^k 中之一同余. 证完.

在第三章 §2 中已经证明，当 $N|O(M)$ 时，Z_M 上共有 $(\varphi(N))^s$ 个不同的 DFT，故又可得

推论 6. 若 $N|O(M)$，则 Z_M 上共有 $(\varphi(N))^{s-1}$ 个含 DFT 的同集类.

综合本节所述，因 $N>1$ 时，常有 $N! \geqslant N > \varphi(N)$，故当

$N|O(M)$ 时：

i）除 $M = p^l$（即 $s = 1$）的情形外，Z_M 上均存在与 DFT 不同集之 CRT，且其个数为 $N!\{(N!)^{s-1} - (\varphi(N))^{s-1}\}$.

ii）对任意 M，Z_M 上均有非 DFT 之 CRT 存在，且其个数为 $(N!)^s - (\varphi(N))^s$.

例. 取 $M = 65 = 5\cdot13$, $N = 4$. 此时模 M 共有 16 个 4 次单位根，它们是 1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64.

由此 16 个 4 次单位根共可作成 $A_{16}^4 = 43680$ 个四元序列 $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$，按(1)式即可作出 43680 个 Z_{65} 上具有循环卷积性质的变换. 而这 43680 个变换中可逆者，即 Z_{65} 上的 CRT 则仅有 $(4!)^2=576$ 个，它们分别属于以下述四元序列为代表的 $(4!)^{2-1}=24$ 个同集类：

(1, 8, 57, 64), (1, 12, 8, 44), (1, 12, 18, 34),
(1, 18, 47, 64), (1, 34, 38, 57), (1, 38, 44, 47),
(8, 12, 14, 31), (8, 14, 51, 57), (8, 27, 44, 51),
(8, 27, 31, 64), (12, 14, 18, 21), (12, 21, 44, 53),
(12, 31, 34, 53), (14, 18, 47, 51), (14, 21, 38, 57),
(14, 31, 38, 47), (18, 21, 27, 64), (18, 27, 34, 51),
(21, 27, 38, 44), (21, 53, 57, 64,) (27, 31, 34, 38),
(31, 47, 53, 64), (34, 51, 53, 57), (44, 47, 51, 53).

在这 24 个同集类中，又有且只有 $(\varphi(4))^{2-1} = 2$ 个是包含 DFT 的，它们分别以四元序列

(1, 8, 57, 64), (1, 18, 47, 64),

即

$$(8^0, 8^1, 8^2, 8^3),\quad (18^0, 18^1, 18^2, 18^3)$$

为代表. 这两个类中各包含 $\varphi(4) = 2$ 个 DFT. 故 Z_{65} 上共有 $(\varphi(4))^2 = 4$个DFT 和 $(4!)^2 - (\varphi(4))^2 = 572$ 个非 DFT 的 CRT.

§4. 二 维 CRT

在第三章 §6 中，曾讨论了二维数论变换，即模 M 剩余类环 Z_M 上的二维 DFT. 现在，我们将如 §2 中所作的那样，把二维 DFT 推广到二维 CRT，同时把在环 Z_M 上的讨论推广到在任意有单位元素的交换环 R 上去讨论. 对与二维 CRT 有关的各种问题(如存在的充分必要条件;正、反变换的具体构造;二维 CRT 与其特例——二维 DFT 的相互关系等)，将给与一般性的解决. 前面关于二维数论变换所得的结果，在这里将作为环 R 取 Z_M、CRT 取 DFT 时之特例而推出.

先引入有关的定义如下:

如在 §2 中那样，仍以 R 表示任意一个有单位元素的交换环.

定义 4. 对环 R 中给定的 $N_1^2+N_2^2$ 个元素 a_{k_1,n_1} 和 b_{n_2,k_2} (n_i, $k_i=0,1,\cdots,N_i-1$; $i=1,2$). 由下面 $N_1\cdot N_2$ 个等式

$$X_{k_1,k_2}=\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}x_{n_1,n_2}a_{k_1,n_1}b_{n_2,k_2} \tag{1}$$

($k_i=0,1,\cdots,N_i-1$, $i=1,2$), 所确定之变 R 上任一长为 $N_1\times N_2$ 的二维序列 x_{n_1,n_2} 为 R 上一个有相同长度的二维序列 X_{k_1,k_2} 的变换，就叫做环 R 上的一个长为 $N_1\times N_2$ 的二维变换.

若以 $\mathbf{A}$, $\mathbf{B}$, $\mathbf{x}$, $\mathbf{X}$ 分别记由 a_{k_1,n_1}, b_{n_2,k_2}, x_{n_1,n_2}, X_{k_1,k_2} 所作成的 N_1 阶, N_2 阶, $N_1\times N_2$ 维, $N_1\times N_2$ 维矩阵，则二维变换(1)可用矩阵表达式

$$\mathbf{X}=\mathbf{A}\mathbf{x}\mathbf{B} \tag{2}$$

表示之. 值得注意的是，变换(1)的矩阵表示式并不唯一，因对环 R 中任一可逆元素 a, 表示式

$$\mathbf{X}=(a\mathbf{A})\mathbf{x}(a^{-1}\mathbf{B})$$

显然与表示式(2)表同样的变换(1).

将(2)转置可得

$$\mathbf{X}'=\mathbf{B}'\mathbf{x}'\mathbf{A}'.$$

显然，它实际上与(2)表示同一个变换(1)，但在形式上却有长度 $N_2 \times N_1$. 故在今后的讨论中，可不失一般性地假定 $N_1 \leqslant N_2$.

定义 5. 环 R 上一个长为 $N_1 \times N_2$ 的二维变换(2)叫做可逆的，如果存在一个变 $\mathbf{X}$ 为 $\mathbf{x}$ 的长为 $N_1 \times N_2$ 的变换 $\mathbf{x} = \mathbf{CXD}$.

定义 6. 环 R 上两个长度同为 $N_1 \times N_2$ 的二维序列

$$\mathbf{x} = \begin{pmatrix} x_{0,0} & \cdots & x_{0,N_2-1} \\ \cdots & \cdots & \cdots \\ x_{N_1-1,0} & \cdots & x_{N_1-1,N_2-1} \end{pmatrix} \text{ 和 } \mathbf{h} = \begin{pmatrix} h_{0,0} & \cdots & h_{0,N_2-1} \\ \cdots & \cdots & \cdots \\ h_{N_1-1,0} & \cdots & h_{N_1-1,N_2-1} \end{pmatrix}$$

的二维循环卷积是指由下式

$$y_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_1,n_2} h_{\langle k_1-n_1\rangle_{N_1}, \langle k_2-n_2\rangle_{N_2}}$$

$$(k_i = 0, 1, \cdots, N_i - 1;\ i = 1, 2),$$

所确定的一个二维序列

$$\mathbf{y} = \begin{pmatrix} y_{0,0} & \cdots & y_{0,N_2-1} \\ \cdots & \cdots & \cdots \\ y_{N_1-1,0} & \cdots & y_{N_1-1,N_2-1} \end{pmatrix}.$$

定义 7. 环 R 上一个长为 $N_1 \times N_2$ 的二维变换(2)叫做具有循环卷积性质的，如果对 R 上任意两个长度同为 $N_1 \times N_2$ 的二维序列 $\mathbf{x}$ 和 $\mathbf{h}$ 以及它们的循环卷积 $\mathbf{y}$，当令 $\mathbf{X} = \mathbf{AxB}$, $\mathbf{H} = \mathbf{AhB}$, $\mathbf{Y} = \mathbf{AyB}$ 时，均有

$$X_{k_1,k_2} \cdot H_{k_1,k_2} = Y_{k_1,k_2}$$

$(k_i = 0, 1, \cdots, N_i - 1;\ i = 1, 2)$.

定义 8. 环 R 上一个长为 $N_1 \times N_2$ 的具有循环卷积性质的可逆二维变换简称为环 R 上的一个长为 $N_1 \times N_2$ 的二维 CRT.

关于二维 CRT 的一个基本结果是下面的定理.

定理 7. 环 R 上一个长为 $N_1 \times N_2$ 的二维变换 $\mathbf{X} = \mathbf{AxB}$ 是环 R 上长为 $N_1 \times N_2$ 的二维 CRT 之充分必要条件是，一维变换 $\mathbf{X}_{N_1 \times 1} = \mathbf{A}\mathbf{x}_{N_1 \times 1}$ 和 $\mathbf{X}_{N_2 \times 1} = \mathbf{B}'\mathbf{x}_{N_2 \times 1}$ 分别是环 R 上长为 N_1 和 N_2 的一维 CRT. 这里，$\mathbf{B}'$ 表示 $\mathbf{B}$ 的转置矩阵，$\mathbf{X}_{N_1 \times 1}$, $\mathbf{x}_{N_1 \times 1}$ 和 $\mathbf{X}_{N_2 \times 1}$,

$\mathbf{x}_{N_2\times 1}$ 分别表示一维序列 X_n, x_n $(n=0,1,\cdots,N_1-1)$ 和 X_k, x_k $(k=0,1,\cdots,N_2-1)$ 所组成之单列矩阵.

在第三章§6中讨论二维数论变换时,由于变换的形状已事先给定,故所需予以确定的仅有 α 和 β 两个数而已. 而在这里,变换矩阵是一般的形式, 需要予以确定的元素 $a_{i,j}$, $b_{i,j}$ 共有 $N_1^2+N_2^2$ 个. 故定理 7 的证明较烦, 这里就不一一写出了. 读者可参看书末所引参考文献 [16].

定理 7 把对任意环 R 上长为 $N_1\times N_2$ 的二维 CRT 的讨论完全地归结为对环 R 上长为 N_1 和 N_2 的两个一维 CRT 的讨论. 因此,前面两节中关于一维 CRT 所得出的一整套结果均可推广到二维 CRT 的情形中去,并得出一整套相应的结果来. 下面,我们择要列出所得之相应结果,且因证明较容易,故均略去.

定理 8. 环 R 上长为 $N_1\times N_2$ 之二维变换 $\mathbf{X}=\mathbf{AxB}$ 是 R 上的一个长为 $N_1\times N_2$ 的二维 CRT 的充分必要条件是,存在 N_1+N_2 个元素 $\alpha_i, \beta_j\in R$ $(i=0,1,\cdots,N_1-1; j=0,1,\cdots,N_2-1)$, 适合

i)

$$\mathbf{A}=\begin{pmatrix}1 & \alpha_0 & \alpha_0^2\cdots & \alpha_0^{N_1-1}\\ \cdots & \cdots & \cdots & \cdots\\ 1 & \alpha_{N_1-1} & \alpha_{N_1-1}^2\cdots & \alpha_{N_1-1}^{N_1-1}\end{pmatrix},\quad \mathbf{B}=\begin{pmatrix}1 & \cdots & 1\\ \beta_0 & \cdots & \beta_{N_2-1}\\ \beta_0^2 & & \beta_{N_2-1}^2\\ \vdots & & \vdots\\ \beta_0^{N_2-1} & & \beta_{N_2-1}^{N_2-1}\end{pmatrix};\quad(3)$$

ii) $\alpha_i^{N_1}=\beta_j^{N_2}=1$ $(i=0,1,\cdots,N_1-1; j=0,1,\cdots,N_2-1)$;

iii) 对 $0\leqslant i_1<i_2\leqslant N_1-1$, $0\leqslant j_1<j_2\leqslant N_2-1$, $\alpha_{i_2}-\alpha_{i_1}$ 和 $\beta_{j_2}-\beta_{j_1}$ 之逆元素均存在.

定理 9. 若定理 8 中的条件成立,则 N_1^{-1}, N_2^{-1} 均必存在, 且

$$\mathbf{A}^{-1}=N_1^{-1}\begin{pmatrix}1 & 1 & \cdots & 1\\ \alpha_0^{-1} & \alpha_1^{-1} & \cdots & \alpha_{N_1-1}^{-1}\\ \cdots & \cdots & \cdots & \cdots\\ \alpha_0^{-(N_1-1)} & \alpha_1^{-(N_1-1)} & \cdots & \alpha_{N_1-1}^{-(N_1-1)}\end{pmatrix},$$

$$\mathbf{B}^{-1} = N_2^{-1}\begin{pmatrix} 1 & \beta_0^{-1} & \cdots \beta_0^{-(N_2-1)} \\ 1 & \beta_1^{-1} & \cdots \beta_1^{-(N_2-1)} \\ \cdots & \cdots & \cdots \\ 1 & \beta_{N_2-1}^{-1} & \cdots \beta_{N_2-1}^{-(N_2-1)} \end{pmatrix}.$$

由此立得下面两个推论：

推论 7. 环 R 上长为 $N_1 \times N_2$ 的二维 DFT 存在的充分必要条件为，存在 $\alpha, \beta \in R$，适合下面的条件：

i) $\alpha^{N_1} = 1$, $\beta^{N_2} = 1$;

ii) 对 $1 \leqslant r \leqslant N_1 - 1$, $1 \leqslant s \leqslant N_2 - 1$, $\alpha^r - 1$ 和 $\beta^s - 1$ 之逆元素均存在.

推论 8. 若推论 7 之条件成立，则必有 N_1^{-1}, N_2^{-1} 存在，且

$$\mathbf{A}^{-1} = N_1^{-1}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(N_1-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{-(N_1-1)} & \cdots & \alpha^{-(N_1-1)^2} \end{pmatrix},$$

$$\mathbf{B}^{-1} = N_2^{-1}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \beta^{-1} & \cdots & \beta^{-(N_2-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{-(N_2-1)} & \cdots & \beta^{-(N_2-1)^2} \end{pmatrix}.$$

定义 9. 设 $\mathbf{X} = \mathbf{A}_i \mathbf{x} \mathbf{B}_i$, $i = 1, 2$, 是环 R 上两个长度相同的二维 CRT. 若 $\mathbf{A}_1$ 和 $\mathbf{A}_2$ 只有行的顺序差异，而 $\mathbf{B}_1$ 和 $\mathbf{B}_2$ 只有列的顺序差异，则称此两个二维 CRT 是同集的.

定理 10. 对给定的正整数 N_1 和 N_2，若在环 R 中二项方程

$$\alpha^{N_1} - 1 = 0 \quad 和 \quad \beta^{N_2} - 1 = 0$$

之根数分别不超过 N_1 和 N_2，则此环 R 上任一长为 $N_1 \times N_2$ 的二维 CRT 均与其上之某一有相同长度的二维 DFT 同集.

取 R 为特定的环 Z_M 可得

定理 8'. 设 $M = p_1^{l_1} \cdots p_t^{l_t}$，则环 Z_M 上长为 $N_1 \times N_2$ 之二维 CRT 存在的充分必要条件为，存在整数 α_i, $\beta_j \in Z_M$ $(i = 0, 1, \cdots, N_1 - 1; j = 0, 1, \cdots, N_2 - 1)$，适合下列条件：

i）变换矩阵具有（3）之形状；

ii）$\alpha_i^{N_1} \equiv \beta_j^{N_2} \equiv 1 \pmod{M}$；

iii）当 $0 \leqslant i_1 < i_2 \leqslant N_1 - 1$，$0 \leqslant j_1 < j_2 \leqslant N_2 - 1$ 时，均有

$$(\alpha_{i_2} - \alpha_{i_1}, p_k) = (\beta_{j_2} - \beta_{j_1}, p_k) = 1 \quad (k = 1, 2, \cdots, s).$$

推论 7′. Z_M 上长为 $N_1 \times N_2$ 之二维 DFT（即二维数论变换）存在的充分必要条件为，存在整数 $\alpha, \beta \in Z_M$，适合下列条件：

i）$\alpha^{N_1} \equiv \beta^{N_2} \equiv 1 \pmod{M}$；

ii）α, β 模 p_k $(k = 1, 2, \cdots, s)$，的次数分别为 N_1 和 N_2.

定理 11. Z_M 上长为 $N_1 \times N_2$ 的二维 CRT 和二维 DFT 存在的充分条件同为

$$[N_1, N_2] \mid O(M),$$

这里，$[N_1, N_2]$ 表示 N_1, N_2 之最小公倍数.

定理 12. 若 $[N_1, N_2] \mid O(M)$，则 Z_M 上共有 $(N_1! \cdot N_2!)^s$ 个不同的长为 $N_1 \times N_2$ 的二维 CRT，分属 $(N_1! \cdot N_2!)^{s-1}$ 个同集类. 其中又共有 $(\varphi(N_1) \cdot \varphi(N_2))^s$ 个不同的二维 DFT，分属 $(\varphi(N_1) \cdot \varphi(N_2))^{s-1}$ 个同集类.

第八章　数论变换在其他方面的应用

前面，我们主要介绍的是用数论变换求整数以及复整数的卷积，在数字处理时要计算这样的卷积运算. 本章将介绍数论变换在大数相乘、$GF(p^n)$ 上的多项式相乘以及 $GF(p)$ 上的多项式相除和求广义 Baker 序列等方面的某些应用.

§1. $GF(p^n)$ 上的多项式相乘

设 $F = GF(p^n)$，则 $F[x]$ 中的多项式

$$f(x) = \sum_{i=0}^{M_1-1} a_i x^i, \qquad g(x) = \sum_{i=0}^{M_2-1} h_i x^i,$$

$$a_i,\ h_j \in F \quad (i = 0, 1, \cdots, M_1 - 1;\ j = 0, 1, \cdots, M_2 - 1)$$

之乘积为

$$e(x) = \sum_{i=0}^{M_1+M_2-2} e_i x^i,$$

$$e_n = \sum_{\substack{0\leqslant k_1\leqslant M_1-1\\ 0\leqslant k_2\leqslant M_2-1\\ k_1+k_2=n}} a_{k_1} h_{k_2} = \sum_{\substack{k_1=0\\ 0\leqslant n-k_1\leqslant M_2-1}}^{M_1-1} a_{k_1} h_{n-k_1}$$

$$(n = 0, 1, \cdots, M_1 + M_2 - 2). \tag{1}$$

(1) 式给出了序列 $a_0, a_1, \cdots, a_{M_1-1}$ 和 $h_0, h_1, \cdots, h_{M_2-1}$ 的(非循环)卷积.

如果有 $N = 2^m \geqslant M_1 + M_2 - 1$，$N | p^n - 1$，就可用 F 上长为 N 的 DFT 来计算这个卷积，否则就要构造出 $F = GF(p^n)$ 的一个扩域 $F' = GF(p^{nl})$，使得 $N | p^{nl} - 1$ 成立，这时才能运用数论变换.

顺便指出，当 $n=1$ 时，即 $F=GF(p)$ 时，可把 $f(x)$, $g(x)$ 的系数视为有理整数，用数论变换求出 e_n，再求 $\langle e_n\rangle_p$ $(n=0, 1, \cdots, M_1+M_2-2)$，便得出了 $f(x)g(x)$ 的系数。

§2. 大整数相乘

设将 a, h 分别表示成 u 进制数

$$a=\sum_{i=0}^{M_1-1} a_i u^i, \quad h=\sum_{i=0}^{M_2-1} h_i u^i,$$

则

$$ah=\sum_{i=0}^{M_1+M_2-2} e_i u^i,$$

e_i 由（1）式给出，但这里的 e_i 不一定满足 $0 \leqslant e_i < u$，故需适当处理才能得出 ah 的 u 进制数表示.

§3. $F=GF(p)$ 上的多项式的除法

设

$$f(x)=\sum_{i=0}^{M_1-1} a_i x^i, \qquad e(x)=\sum_{i=0}^{M_1+M_2-2} e_i x^i$$

$(M_1>2, M_2 \geqslant 2)$，$a_i, e_j \in F$ $(i=0, 1, \cdots, M_1-1;\ j=0, 1, \cdots, M_1+M_2-2)$，其中 $f(x)$ 是 F 上的不可约多项式，我们需要判断

$$f(x) \mid e(x) \quad 或 \quad f(x) \nmid e(x),$$

如果 $f(x) \mid e(x)$，则求出商

$$g(x)=\sum_{i=0}^{M_2-1} h_i x^i.$$

方法是选择 N 和 n 适合

$$N=2^m \geqslant M_1+M_2-1, \quad 2^m \mid p^n-1, \quad M_1-1 \nmid n.$$

令

$$a_0, a_1, \cdots, a_{M_1-1}, a_{M_1} = a_{M_1+1} = \cdots = a_{N-1} = 0,$$

$$e_0, e_1, \cdots, e_{M_1+M_2-2}, e_{M_1+M_2-1} = e_{M_1+M_2} = \cdots = e_{N-1} = 0,$$

再设

$$E_k = \sum_{n=0}^{N-1} e_n \alpha^{nk} \quad (k = 0, 1, \cdots, N-1),$$

$$A_k = \sum_{n=0}^{N-1} a_n \alpha^{nk} \quad (k = 0, 1, \cdots, N-1),$$

$\alpha \in GF(p^n)$ 是 2^m 次本原单位根。由于

$$A_k = f(\alpha^k) \quad (k = 0, 1, \cdots, N-1),$$

故 $A_k \neq 0$ $(k = 0, 1, \cdots, N-1)$，否则将存在某一个 k，有 $A_k = 0$，设 $\alpha^k = \beta$，我们有

$$\left\{\sum_{i=0}^{M_1-2} t_i \beta^i \mid t_i \in GF(p) \ (i = 0, 1, \cdots, M_1 - 2)\right\} = GF(p^{M_1-1}),$$

是 $GF(p^n)$ 的一个子域，这与 $M_1 - 1 \nmid n$ 矛盾。故可令

$$H_k = E_k \cdot A_k^{-1} \quad (k = 0, 1, \cdots, N-1),$$

而用数论变换求出

$$h_n = N^{-1} \sum_{k=0}^{N-1} H_k \alpha^{-nk}$$

$$(n = 0, \cdots, M_2 - 1, M_2, \cdots, N-1),$$

因为 $f(x) \mid e(x)$ 与否和 $F = GF(p)$ 或 $F = GF(p^n)$ 无关，所以 $f(x) \mid e(x)$ 的充分必要条件是 $h_{M_2} = \cdots = h_{N-1} = 0$。且当 $h_{M_2} = \cdots = h_{N-1} = 0$ 时，$\displaystyle\sum_{i=0}^{M_2-1} h_i x^i = \frac{e(x)}{f(x)}$.

§4. 计算序列的相关函数

本节将指出，两个周期序列的互相关函数可化为求序列的循环卷积，从而也提供了寻找广义 Baker 序列的一个方法，因 Baker 序列取 1 或 −1 两个值，这时数论变换的选择将比较容易。

设 $a_0, a_1, \cdots, a_{N-1}$; $b_0, b_1, \cdots, b_{N-1}$ 是两个周期为 N 的序列，即 $a_{i+N} = a_i$, $b_{i+N} = b_i$, 其互相关函数定义为

$$B(L) = \sum_{i=0}^{N-1} a_i b_{i+L} \quad (L = 0, 1, \cdots, N-1).$$

如果 $a_i = b_i (i = 0, 1, \cdots, N-1)$, 则称上式为 $a_0, a_1, \cdots, a_{N-1}$ 的自相关函数. 今作序列 $x_n = a_{N-n}$, $h_n = b_n$ $(n = 0, 1, \cdots, N-1)$, 求其循环卷积得

$$y_L = \sum_{k=0}^{N-1} x_k h_{\langle L-k \rangle_N} = \sum_{k=0}^{N-1} a_{N-k} h_{\langle L+N-k \rangle_N}$$

$$= \sum_{t=0}^{N-1} a_t h_{\langle L+t \rangle_N} = \sum_{t=0}^{N-1} a_t b_{L+t}$$

$$(L = 0, 1, \cdots, N-1),$$

故得 $B(L) = y_L$ $(L = 0, 1, \cdots, N-1)$.

现在设 $a_0, a_1, \cdots, a_{N-1}$ 为非周期有限序列，且 $a_i = 1$ 或 -1 $(i = 0, 1, \cdots, N-1)$, 其自相关函数定义为

$$C(L) = \sum_{k=0}^{N-1-L} a_k a_{k+L} \quad (L = 0, 1, \cdots, N-1).$$

如果 $|C(L)| \leqslant 1$ $(L = 1, 2, \cdots, N-1)$, 则序列 $a_0, a_1, \cdots, a_{N-1}$ 就称为 Baker 序列. 如果

$$|C(L)| \leqslant u, \ u \geqslant 2 \ (L = 1, 2, \cdots, N-1),$$

此时 $a_0, a_1, \cdots, a_{N-1}$ 就称为广义 Baker 序列.

现在设 $x_i = a_i (i = 0, 1, \cdots, N-1)$, $x_j = 0$ $(j = N, \cdots, 2N-2, \cdots, 2^s - 1)$[1], 这里 s 满足 $2^s \geqslant 2N-1 > 2^{s-1}$, 并将此序列作周期为 2^s 的延拓，即设 $x_{k+2^s} = x_k$, 求其自相关函数，并令 $L = 1, 2, \cdots, N-1$ 可得

$$B(L) = \sum_{k=0}^{2^s-1} x_k x_{k+L} = \sum_{k=0}^{N-1} x_k x_{k+L}$$

[1] 因为要用数论变换作快速演段，一般将序列延长到 $2^s - 1$, 实际延长到 $2N-2$ 就行了.

$$= \sum_{k=0}^{N-1-L} x_k x_{k+L} + \sum_{k=N-L}^{N-1} x_k x_{k+L}$$

$$= \sum_{k=0}^{N-1-L} x_k x_{k+L} = \sum_{k=0}^{N-1-L} a_k a_{k+L} = C(L)$$

目前，对这类广义的 Baker 序列基本上没有一般性的结果，只能在电子计算机上用“穷举法”逐个检验其自相关函数. 易知，其全部乘、加法次数的阶是 $O(N^2)$，随着N的增大，计算量急剧增加，要判定有无长为 N 的广义的 Baker 序列是非常困难的. 如果采用上述的方法，用数论变换来计算，则所需乘、加法次数的阶可降为 $O(N\log_2 N)$，这是因为

$$2^s \geqslant 2N-1 > 2^{s-1}.$$

故用数论变换作快速演段(与 FFT 一样)所需的全部乘、加法次数大致为

$$3\cdot s\cdot 2^s + 2^s < 2(2N-1)[3\log_2 2(2N-1)+1]$$
$$= O(N\log_2 N).$$

参 考 文 献

[1] 华罗庚，数论导引，科学出版社，1957.
[2] 闵嗣鹤、严士健，初等数论，高等教育出版社，1957.
[3] 万哲先，代数和编码，科学出版社，1976.
[4] B. L. 范德瓦尔登，代数学 (I)，科学出版社，1963.
[5] 燃料化学工业部石油地球物理勘探局计算中心站等，地震勘探数字技术(第一册)，科学出版社，1974.
[6] Dickson, L. E., History of the Theory of Numbers, Vol. 1, Washington, D. C., Carnegie Institute, 1919.
[7] Gold, B. and Rader, C. M., Digital Processing Signals, New York, McGraw-Hill, 1969.
[8] 数丁，数论变换(一)，数学的实践与认识，**3** (1977)，45—52.
[9] 数丁，数论变换(二)，数学的实践与认识，**4** (1977)，47—56.
[10] 数丁，数论变换(三)，数学的实践与认识，**2** (1978)，69—81.
[11] 数丁，关于数论变换，«关于数论变换»一文的补充，四川大学学报(自然科学版)，**3** (1976)，1—10.
[12] 孙琦、郑德勋、沈仲琦，在二次域 $R(\sqrt{m})$ 的整数剩类环里计算卷积，四川大学学报(自然科学版)，**1** (1978)，1—10.
[13] 沈仲琦、孙琦、郑德勋，关于 Z_M 上二维 DFT 的一点注记，四川大学学报(自然科学版)，**2—3** (1978)，1—3.
[14] 郑德勋、孙琦、沈仲琦，关于具有循环卷积性质的可逆变换，四川大学学报(自然科学版)，**4** (1978)，1—12.
[15] 孙琦，关于分圆域的整数剩余类环上的 DFT，四川大学学报 (自然科学版)，**4** (1978)，13—18.
[16] 郑德勋、孙琦、沈仲琦，任意环上具有循环卷积性质的二维可逆变换，四川大学学报(自然科学版)，**3** (1979)，19—30.
[17] 戚征，伪随机序列，数学的实践与认识，**7** (1972)，26—45.
[18] Agrawal, R. C., Burrus, C. S., Fast Digital Convolution Using Fermat Transforms, *SWIEEECO, Record,* 1973, 538—543.
[19] Agarwal, R. C., Burrus. C. S., Fast Convolution Using Fermat Number Transforms with Application to Digital Filtering, *IEEE Trans.,* Acoustics, Speech, and Signal Processing, **22**(1974), 87—97.
[20] Agarwal, R. C., Burrus, C. S., Number Theoretic Transforms to Implement Fast Digital Convolution, *PIEEE,* **63**(1975), 550—560.
[21] McClellan, J. H., Hardware Realization of a Fermat Number Transform, *IEEE Trans.,* Acoustics, Speech, and Signal Processing, **24**(1976), 216—225.
[22] Pollard, J. M., The Fast Fourier Transform, *Math. Comput.,* **25**

(1971), 365—374.

[23] Leibowitz, I. M., A Simplified Binary Arithmetic for the Fermat Number Transform, *IEEE Trans.*, Acoustics, Speech, and Signal Processing, **24**(1976), 356—359.

[24] Reed, I. S., Truong, T. K., The Use of Finite Fields to Compute Convolutions, *IEEE Trans.*, Inform. Theory, **21**(1975), 208—213.

[25] Reed, I. S., Truong, T. K., Complex Integers Convolutions over a Direct Sum of Galois Fields, *IEEE Trans.*, Inform. Theory, **21**(1975), 657—661.

[26] Reed, I. S., Truong, T. K., Convolutions over Residue Classes of Quadratic integers, *IEEE Trans.*, Inform. Theory, **22**(1976), 468—475.

[27] Agrwal, R. C., Burrus, C. S., Fast Ine-dimensional Digital convolution by Multi-dimensional Techniques, *IEEE Trans.*, Acoustics, Speech, and Signal Processing, **22**(1974), 1—10.

[28] Rader, C. M., On the Application of the Number Theoretic Transforms of High Speed Convolution Two-dimensional Filtering, *IEEE Trans.*, Circuits and Systems, **22**(1975), 575.

[29] Rader, C. M., Discrete Convolution via Mersenne Transforms, *IEEE Trans., Comput.*, **21**(1972), 1269—1273.

[30] Golomb, S. W., Properties of the Sequence $3\cdot 2^n+1$, *Math. Comp.*, **30** (1976).

[31] Silverman H. F. On Introduction to Programming the Winograd Fourier Transform (WFTA), *IEEE Trans.*, Acoustics, Speech, and Signal Processing,**25**(1977), 152—165.

[32] Hardy, G. H., Wright, E. M., An Introduction to the Theory of numbers, 3rd edition. Oxford, 1954.

[33] Mann, H. B., Introduction to Algebraic Number Theory, Columbus, Ohio State Univ. Press, 1955.

[34] 孙琦，关于长为 $2p^l$ 的离散傅里叶变换，四川大学学报(自然科学版)，**2**(1979)，65—70.

[35] 孙琦，关于代数数域 $R(\theta)$ 的整数剩余类环上的DFT 及其他，四川大学学报(自然科学版)，**3**(1979)，11—18.

[General Information]
书名=快速数论变换
作者=孙琦　　郑德勋　沈仲琦
页数=205
SS号=10236747
DX号=
出版日期=1980年10月第1版
出版社=科学出版社

封面
书名
版权
前言
目录
第一章 初等数论
1.整数的分解
2.同余式
3.二次剩余
第二章 卷积运算和快速变换
1.卷积运算
2.DFT
3.FFT
4.素数幂变换
5.WFTA
第三章 数率变换的理论基础
1.数论变换和快速数论变换
2.数论变换的具体构造
3.Fermat数变换
4.用快速数论变换计算循环卷积
5.三项式变换
6.二维数论变换
7.用二维快速数论变换计算一维卷积
8.多维数论变换
9.用孙子定理减少字长
第四章 Fermat数变换实现中的若干问题
1.流向图与蝶件
2.计算机上膜Ft运算的实现
3.字长与序列长度间的关系
4.用快速Fermat数变换与FFT计算卷积运算量的比较
第五章 代数数论初步
1.环和域

2.代数数和代数数域
3.R(θ)的基底和整底
4.整除性和素数
5.理想数，同余
6.二次域R(？)
7.属于不同域的理想数
8.素理想数的一些性质
9.［p］的分解
10.在分圆域上［p］的分解
第六章 二次域和分圆域内的DFT构造
1.计算复整数序列的卷积
2.在二次域R(？)里计算卷积
3.在分圆域里计算卷积
第七章 任意环上具有循环卷积性质的可逆变换
1.引言
2.任意环上的CRT
3.ZM上的CRT
4.二维CRT
第八章 数论变换在其他方面的应用
1.GF(pn)上的多项式相乘
2.大整数相乘
3.F=GF(p)上的多项式的除法
4.计算序列的相关函数
参考文献